



# HIPAA COMPLIANCE REVIEW DRAGON MEDICAL V 10

CSC  
3811 Turtle Creek Blvd  
Suite 2000  
Dallas, TX 75219  
Phone: 214.520.0555





# TABLE OF CONTENTS

<b>1.0 Introduction</b>	<b>1</b>
<b>2.0 Findings</b>	<b>1</b>
2.1 Observations and Recommendations	1
2.2 HIPAA Matrix	2

# DRAGON MEDICAL V10: HIPAA COMPLIANCE REVIEW

## 1.0 Introduction

Nuance has released version 10 of Dragon Medical and, in preparation for this release, has engaged CSC to provide an independent review of Dragon Medical's compliance with the HIPAA Security Rule. CSC is a leading provider of healthcare information technology strategy and clinical implementation practices for providers in all healthcare settings. As part of its review, CSC has published this white paper which validates and outlines the HIPAA security considerations designed into the software.

## 2.0 Findings

Assessment activities included question/answer sessions with Dragon Medical architects and engineers and review of the following product documentation:

- User Guide: Dragon Medical Enterprise Version 10
- User Guide: Dragon Medical Preferred Version 10
- Optimizing Clinical Productivity: Using Speech Recognition with Medical Features vs. a General Purpose Solution (White Paper)
- Dragon Medical Network and Security Issues (February 7, 2008)

### 2.1 Observations and Recommendations

Dragon Medical is speech recognition software that automates the input of text and commands into the user interface of any application including Microsoft Word, PowerPoint, Internet Explorer, Mozilla Firefox, and most major Electronic Health Record (EHR) systems, replacing manual input via the keyboard and mouse peripherals.

CSC evaluated Dragon Medical Version 10 against the Administrative, Physical, and Technical Safeguards established by the Department of Health and Human Services in §164.308, §164.310, and §164.312 of the Healthcare Insurance Reform: Security Standards; Final Rule.

The evaluation determined that Dragon Medical has a minimum amount of security built into the product, relying instead on security mechanisms provided by the Windows operating system (O/S) on which it resides and other third-party applications.

## 2.2 HIPAA Matrix

<b>Administrative Safeguards</b>	
<b>Standard and Specification</b>	<b>Dragon Naturally Speaking</b>
<b>Security Management Process</b>	
<i>Risk Analysis (R)</i>	Through the creation of a HIPAA Compliance whitepaper, Nuance can provide security-related details that can assist an institution in completing a HIPAA risk analysis of the Dragon Medical product line.
<i>Risk Management (R)</i>	Dragon Medical has a minimum amount of security built into the application. Instead, the product relies on the security mechanisms found in the Windows operating system (O/S) on which it resides and other third-party applications to manage security risks.
<i>Sanction Policy (R)</i>	No applicable feature found
<i>Information System Activity Review (R)</i>	No applicable feature found
<b>Assigned Security Responsibility (R)</b>	No applicable feature found
<b>Workforce Security</b>	
<i>Authorization and/or Supervision (A)</i>	Dragon Medical supports a 'PUSH' installation method where the organization can control distribution of the application and push it out to only those workstations pre-authorized by management to have it.  The ability to modify the application's configuration on Windows NT, 2000, XP & Vista systems formatted as NTFS depends on whether or not the user has O/S administrative privileges.
<i>Workforce Clearance Procedures (A)</i>	No applicable feature found
<i>Termination Procedures (A)</i>	No applicable feature found
<b>Information Access Management</b>	
<i>Isolating Healthcare Clearinghouse Functions (R)</i>	N/A
<i>Access Authorization (A)</i>	Dragon Medical relies on Windows file permissions to control access to directories and files containing sensitive information.
<i>Access Establishment and Modification (A)</i>	Depending on the operating system (O/S), the user's ability to modify the application setup would depend on whether or not they had administrative privileges at the O/S level.

<b>Administrative Safeguards</b>	
<b>Standard and Specification</b>	<b>Dragon Naturally Speaking</b>
<b>Security Awareness and Training</b>	
<i>Security Reminders (A)</i>	The Dragon Medical administration guide and periodic information articles sent to customers provide security related recommendations and instructions.
<i>Protection from Malicious Software (A)</i>	Dragon Medical can coexist on systems with virus protection software with no impact to functionality.
<i>Log-in Monitoring (A)</i>	No applicable feature found
<i>Password Management (A)</i>	Dragon Medical is not password protected when access locally at the workstation. Roaming users accessing a Dragon network server can be forced to authenticate by Windows file permissions and/or WebDAV.
<b>Security Incident Response</b>	
<i>Response and Reporting (R)</i>	The Dragon Medical logging feature records a variety of information to assist in the identification and response to suspicious activity and events.
<b>Contingency Plan</b>	
<i>Data Backup Plan (R)</i>	Dragon Medical automatically creates a backup copy of each non-roaming user file. Automatic backup of user profiles is not available for non-roaming and roaming profiles stored on a network drive – the client must implement a separate backup process.
<i>Disaster Recovery Plan (R)</i>	Disaster Recovery procedures for Dragon Medical can be crafted from standard Windows file disaster recovery technologies, strategies and third party solutions.
<i>Emergency Mode Operations Plan (R)</i> <i>Testing and Revision Procedures (A)</i> <i>Application and Data Criticality Analysis (A)</i>	Dragon Medical is compatible with data backup and disk imaging products that are certified to work with the current Windows desktop and server operating systems.
<b>Evaluation</b>	
<i>Response and Reporting (R)</i>	Nuance continually reviews customer requests for security features and enhancements based upon the results of internal risk assessment activities.
<b>Business Associate Contract and Other Arrangements</b>	
<i>Written Contract or Other Arrangements (R)</i>	N/A

<b>Physical Safeguards</b>	
<b>Standard and Specification</b>	<b>Dragon Naturally Speaking</b>
<b>Facility Access Controls</b>	
<i>Contingency Operations (A)</i> <i>Facility Security Plan (A)</i> <i>Access Control and Validation (A)</i> <i>Procedures (A)</i> <i>Maintenance Records (A)</i>	N/A
<b>Workstation Use (R)</b>	N/A
<b>Workstation Security (R)</b>	Dragon Medical relies on standard Windows workstations security features (e.g. user login, password protected screensaver) and directory/file permissions to deter unauthorized access to the application and associated files.
<b>Device and Media Controls</b>	
<i>Disposal (R)</i> <i>Media Reuse (R)</i> <i>Accountability (R)</i> <i>Data Backup and Storage (R)</i>	N/A

<b>Technical Safeguards</b>	
<b>Standard and Specification</b>	<b>Dragon Naturally Speaking</b>
<b>Access Control</b>	
<i>Unique User Identification (R)</i>	Relies on the Windows security controls and directory/file permissions to authenticate users. There is no additional authentication required by NaturallySpeaking.  When utilizing the Master Roaming User feature, authentication to the centralized Dragon server is enforced by Windows file permissions or HTTP Roaming with WebDAV.
<i>Emergency Access Procedures (R)</i>	No feature identified
<i>Automatic Logoff (A)</i>	No feature identified

<b>Technical Safeguards</b>	
<b>Standard and Specification</b>	<b>Dragon Naturally Speaking</b>
<i>Encryption and Decryption (A)</i>	When the Language Model Optimizer feature is enabled, Dragon Medical automatically retains and encrypts a subset of audio and text files on the local machine using Microsoft Windows cryptography. Although Dragon Medical does not automatically encrypt the audio and text files dictated into another application such as MS Word, the user can protect the confidentiality and integrity of the information by implementing a separate file-level encryption solution without impacting Dragon Medical functionality.
<i>Audit Controls (R)</i>	The Dragon Medical logging feature captures a variety of information to assist in auditing user activities including targeted applications, changes to user profiles, and words added to the speech recognition profile.
<b>Integrity</b>	
<i>Mechanisms to Authenticate ePHI (A)</i>	No feature identified
<i>Person or Entity Authentication (R)</i>	Dragon Medical relies on Windows security controls and file permissions to authenticate users.
<b>Transmission</b>	
<i>Integrity Control (A)</i> <i>Encryption (A)</i>	Dragon Medical support HTTP over Secure Sockets Layer (SSL) when the Roaming User feature is enabled.

## **CSC**

Turtle Creek Centre  
3811 Turtle Creek Blvd.  
Suite 2000  
Dallas, TX, 75219  
+1.214.520.0555

### **Worldwide CSC Headquarters**

#### **The Americas**

3170 Fairview Park Drive  
Falls Church, Virginia 22042  
United States  
+1.703.876.1000

#### **Europe, Middle East, Africa**

Royal Pavilion  
Wellesley Road  
Aldershot  
Hampshire GU11 1PZ  
United Kingdom  
+44(0)1252.534000

#### **Australia**

26 Talavera Road  
Macquarie Park, NSW 2113  
Australia  
+61(0)29034.3000

#### **Asia**

139 Cecil Street  
#08-00 Cecil House  
Singapore 069539  
Republic of Singapore  
+65.221.9095

### **About CSC**

*The mission of CSC is to be a global leader in providing technology enabled business solutions and services.*

*With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.*

*CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.*

*For more than 45 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.*

*The company trades on the New York Stock Exchange under the symbol "CSC."*

© 2008 Computer Sciences Corporation.

