

Support for the HIPAA Security Rule PowerScribe® for Radiology 5.0 System

SUMMARY

This whitepaper is intended to assist Nuance® customers who are evaluating the security aspects of the PowerScribe® system as part of their risk analysis required for Health Information Portability and Accountability Act (HIPAA) Security Rule compliance. The paper describes specific features of the PowerScribe system in the context of the security standards and provides an analysis on how the system can support an organization's efforts to attain HIPAA Security Rule compliance. Nuance Communications understands that compliance presents a significant challenge confronting our customers. We continue to enhance PowerScribe product features and services to address security and compliance efforts of our customers.

HIPAA Security Rule Compliance

The HIPAA Security Rule ("the rule") was published with the intent to protect the confidentiality, integrity and availability of electronic protected health information (ePHI). The rule defined in 45 CFR Parts 160, 162 and 164 establishes the minimum national standards for information systems with access to ePHI. PowerScribe manages and stores ePHI as dictations and medical reports in an electronic form and thus must be included in the risk assessment activities of our customers pursuant to HIPAA Security Rule compliance. Compliance with the rule is required no later than April 21, 2005. Small health plans must comply no later than April 21, 2006.

The rule establishes a minimum set of administrative, technical and physical standards and implementation specifications which must be addressed. However, it is written in terms that are "as generic as possible and which, generally speaking, may be met through various approaches or technologies."¹ Thus the rule is not prescriptive. "The steps an institution will actually need to take to comply with these regulations will be dependent upon its own particular environment and circumstances and risk assessment."² An Institution cannot simply purchase HIPAA certified hardware or software to achieve compliance. Rather, it must implement policies and procedures which are consistent with the rule and evaluate technology decisions based upon a risk assessment process. "The standards do not allow organizations to make their own rules, only their own technology choices."³

HIPAA is flexible. According to the rule, "Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." What is reasonable and appropriate is based upon the findings of a risk assessment which considers size, complexity, capability, technical infrastructure, probability of risk, criticality of data and cost of the security measure. In other words, an institution must demonstrate that its choices are reasonable and appropriate given the cost and the benefit.

Dictaphone® PowerScribe for Radiology 5.0 system was introduced to the market in June 2008 as a web-enabled dictation system with completely integrated transcription functionality. The product is considered mature and many of its features have been refined over the past 10 years to meet complex customer needs. The application is designed to capture dictated audio and use speech recognition to generate text reports in order-centric environments.

¹Federal Register / Vol. 68, No. 34, pp 8336

²IBID

³Federal Register / Vol. 68, No. 34, pp 8343

The paper provides a brief analysis of how PowerScribe supports an organization's efforts to comply with HIPAA's Security Rule standards. The datasheet describes HIPAA-related security features in the latest versions of software and includes the following product components:

PowerScribe for Radiology 5.0

- Dictation/Correction Client
- Order/Entry Client
- Administrator Client
- Coding Manager

The PowerScribe system contains multiple levels of system security to protect patient confidentiality and user or group privileges that grant or restrict access to specific product features. The system is equipped with comprehensive audit and reporting capabilities to provide details related to documentation creation, users, editors, signers, timestamps, viewing, distribution, etc.

PowerScribe HIPAA Security Rule Compliance Features/Offering

Nuance Communications, in collaboration with an independent consulting firm specializing in IT security and the HIPAA Security Rule, conducted an assessment of Dictaphone's PowerScribe system and developed this white paper. The paper describes HIPAA-related security features in the above mentioned versions of PowerScribe software; however, it does not discuss security features in previously released versions. The following table identifies the HIPAA standards, implementation specifications, marks each implementation specification as required (R) or addressable (A) and identifies the key PowerScribe product features which will complement efforts to achieve HIPAA Security Rule compliance. The PowerScribe system features alone do not ensure HIPAA Security Rule compliance and are only features that may be useful as the customer takes steps toward compliance.

ADMINISTRATIVE SAFEGUARDS

Security Management Process

Standard and Specification	PowerScribe® Feature/Offering
Risk Analysis (R)	This datasheet provides details intended to assist an institution in completing a HIPAA risk analysis of the PowerScribe product
Risk Management (R)	The PowerScribe product includes a number of configurable security measures that improve an institution’s ability to manager risks and vulnerabilities. These security measures include user and password management, session encryption, audit and logging mechanisms, and configurable workflow processes that can improve data integrity.
Sanction Policy (R)	Passwords can be administratively changed to revoke access in support of a sanction policy. User accounts can be administratively disabled to revoke access in support of a sanction policy
Information System Activity Review (R)	Various audit reports provide information vital to implementing Information System Activity Review specifications.
Assigned Security Responsibility (R)	Dictaphone has a dedicated Manager of Information Security who is responsible for internal security policy. Two levels of authority, Administrator and System Administrator, are provided for administration the various security mechanisms featured in the PowerScribe system.

Workforce Security

Standard and Specification	PowerScribe® Feature/Offering
Authorization and/or Supervision (A), Workforce Clearance Procedures (A)	PowerScribe’s role-based user groups can be easily incorporated into the access authorization and workforce clearance processes/ procedures that an institution implements to determine appropriate access to protected information.
Termination Procedures (A)	Passwords can be administratively changed to revoke access in support of termination procedures. User account can be administratively disabled or completely removed to revoke access in support of termination procedures.

Information Access Management

Standard and Specification	PowerScribe® Feature/Offering
<p>Isolating Healthcare Clearinghouse Functions (R), Access Authorization (A)</p>	<p>PowerScribe helps support the access authorization specifications by providing the capability to implement centralized role based on security through the use of groups that can be created based on roles, departments, geographic locations or any other identifying criteria with each group and its accompanying users being granted unique user rights and privileges.</p>
<p>Access Establishment and Modification (A)</p>	<p>PowerScribe provides a comprehensive capability to create and manage user accounts and associated roles and privileges via two levels of administration (Administrators, System Administrators) which have groupings of functions applied to each administrative level. The following roles can be added or revoked by administrators depending on their privileges, per group or user:</p> <ul style="list-style-type: none"> • Author - enables report authors to the Dictation/Correction Client to dictate reports. • Editor - enables report editors access to the Dictation/Correction Client for editing and correction of dictated reports. • Order/Visit Entry - enables access to the Order Entry application to enter new patients and orders into PowerScribe Workstation. • Administrator - enables access to perform administrator functions. • System Administrator - enables access to perform system administrator functions. <p><i>Note: See PowerScribe Admin Guide for privileges associated with roles.</i></p>

Security Awareness and Training

Standard and Specification	PowerScribe® Feature/Offering
Security Reminders (A)	<p>The PowerScribe administration guide and periodic information articles sent to customers provide security related recommendations and instructions. The Dictaphone Consulting Group (DCG) can also be contracted to provide installation and/or operational process and procedural expert guidance to support customer's unique implementation requirements and training activities.</p>
Protection from Malicious Software (A)	<p>PowerScribe is certified to work with the following anti-virus packages:</p> <ul style="list-style-type: none"> • Symantec™ Norton Antivirus™ • McAfee® (known to work but not certified)
Log-in Monitoring (A)	<p>The Login Manager can be used to monitor all non-administrative users using the system. Inactive users can be immediately logged out. The following login statistics can be viewed at any time:</p> <ul style="list-style-type: none"> • User ID - the user's unique User ID • Login ID - the user's Login ID • Name - the user's name • Start Login - the date and time the user began the current login session. • Remote - the name of the user's client machine • Last - the time of the user's last logout or the current time, if the user is still logged in. <p><i>Note: Remote and Last statistics are not available in the Encounters user interface.</i></p>
Password Management (A)	<p>The following password management features are available:</p> <ul style="list-style-type: none"> • Masked password entry • Password aging and forced expiration • Administrative password reset and change • Settable minimum password length • Password encrypted in storage

Security Incident Response

Standard and Specification	PowerScribe® Feature/Offering
Response and Reporting (R)	PowerScribe Login Manager, Report Manager and Crystal Reports reporting engine can be utilized in responding to incidents and supports the forensics and investigation processes by generating very detailed standard or custom reports. Reports can also be exported for additional processing and analysis.

Contingency Plan

Standard and Specification	PowerScribe® Feature/Offering
Data Backup Plan (R)	Backups of critical PowerScribe files can be made with any software which can successfully handle SQL Server databases and Windows open files. PowerScribe has been tested with the following backup product: <ul style="list-style-type: none"> • Veritas Backup Exec
Disaster Recovery Plan (R)	Disaster Recovery procedures for PowerScribe can be crafted which are based upon standard Windows and SQL Server disaster recovery technologies, strategies and third party solutions. Dictaphone supports a customer supplied clustered SQL architecture or cold standby servers.
Emergency Mode Operations Plan (R) Testing and Revision Procedures (A)	PowerScribe is compatible with backup and disk imaging products that are certified to work with the current Windows® desktop and server operating systems.
Application and Data Criticality Analysis (A)	

Evaluation

Standard and Specification	PowerScribe® Feature/Offering
Response and Reporting (R)	Dictaphone continually review customer requests for security features and enhancements based upon the results of internal risk assessment activities.

Business Associate Contract and Other Arrangements

Standard and Specification	PowerScribe® Feature/Offering
Written Contract or Other Arrangements (R)	Nuance will execute HIPAA Business Associate Agreements with its customers who purchase Maintenance, iChart or other services.

PHYSICAL SAFEGUARDS

Facility Access Controls

Standard and Specification	PowerScribe® Feature/Offering
Contingency Operations (A)	N/A
Facility Security Plan (A)	
Access Control and Validation (A)	
Procedures (A)	
Maintenance Records (A)	

Workstation Use (R)

N/A

Workstation Security (R)

PowerScribe uses standard Windows workstations which support a variety of physical security mechanisms. PowerScribe supports session termination after a specified time of inactivity.

Device and Media Controls

Standard and Specification	PowerScribe® Feature/Offering
Disposal (R)	N/A
Media Reuse (R)	
Accountability (R)	
Data Backup and Storage (R)	

TECHNICAL SAFEGUARDS

Access Control

Standard and Specification	PowerScribe® Feature/Offering
Unique User Identification (R)	The PowerScribe system fully supports the creation, maintenance and use of unique user identifiers. The system can be configured to require an additional user identifier to sign a report. PowerScribe also supports standard LDAP services to authenticate users (username/password)
Emergency Access Procedures (R)	Administrator accounts can be used to provide full access to system features in the event of an emergency.
Automatic Logoff (A)	PowerScribe has a configurable inactivity timeout feature that can be utilized to automatically logoff idle users within the application.
Encryption and Decryption (A)	Third party encryption and decryption solutions can be used at the customer's discretion but are not supported by PowerScribe.
Audit Controls (R)	<p>In addition to the standard audit and logging features found in a Windows operating system and SQL server database system, PowerScribe includes a robust auditing feature that records activities performed by administrators and users of the PowerScribe system. Log files capture detailed information concerning the activities performed in each of the PowerScribe application areas — Administrator (ADM), PowerScribe API (API), Dictation/Correction (DC), Order Entry (OE), Telephony (TEL), System (SYS), and Coding Manager (CM).</p> <p>The following information is captured for every event:</p> <ul style="list-style-type: none"> • Date and time • Computer name or IP address • Application area • User name • Description of event <p>Other activities recorded include:</p> <ul style="list-style-type: none"> • Access failures (e.g. incorrect username or password, incorrect privileges) • User logins and logouts • Password changes • Add, modify, delete users and groups • System parameter changes • Patient information created or updated • Reports created, edited, or deleted • Reports signed or returned • Reports faxed or printed • Report property changes • Notes viewed

Integrity

Standard and Specification	PowerScribe® Feature/Offering
<p>Mechanisms to Authenticate ePHI (A)</p>	<p>PowerScribe utilized both application and operating system features to restrict access rights to authorized users as a preventative integrity control. Application and operating system audit logs can be used to track the activity of authorized users and detect the activity of unauthorized users as a detective integrity control. Purging of audio and text files is system configurable as the administrative level and can be totally disabled. Configurable workflow processes can be implemented to facilitate integrity checking by requiring transcribed reports to be reviewed for accuracy prior to being signed.</p>
<p>Person or Entity Authentication (R)</p>	<p>PowerScribe is compatible with all Windows-based biometric and multi-factor authentication schemes when they are used as prescribed by the vendor. PowerScribe support Lightweight Directory Access Protocol (LDAP) for those institutions that leverage LDAP services to authenticate users.</p>

Transmission

Standard and Specification	PowerScribe® Feature/Offering
<p>Integrity Control (A) Encryption (A)</p>	<p>PowerScribe supports Secure Sockets Layer (SSL) communication between clients and servers to protect data integrity and data confidentiality. When SSL is not enabled, PowerScribe relies upon lower level integrity and encryption services such as VPN, Windows operating system and TCP/IP network devices for transmission security.</p>

The experience speaks for itself™

NUANCE COMMUNICATIONS, INC.

ONE WAYSIDE ROAD
BURLINGTON, MA 01803

888 350 4836
NUANCE.COM

