Support for the HIPAA Security Rule
PowerScribe® System

Summary
This whitepaper is intended to assist Dictaphone 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. Dictaphone understands that compliance presents a significant short-term 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.

The contents of this White Paper are general in nature. These contents constitute neither a legal opinion nor a representation about whether the Dictaphone products and services will ensurethat any individual healthcare provider meets its HIPAA compliance obligations.
[1]Federal Register / Vol. 68, No. 34, pp 8336 [2]IBID [3]Federal Register / Vol. 68, No. 34, pp 8343

PowerScribe Overview
Dictaphone's PowerScribe system was introduced to the market in December 2002 as a client/server web-based dictation system with completely integrated transcription functionality. The product is considered mature and many of its features have been refined over the years to meet complex customer needs. The application is designed to capture dictated audio and use speech recognition to generate text reports in an encounter or order-centric (for example, Radiology, Emergency Medicine) environment.
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 .
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 provides dictation redundancy software and hardware configurations that support disaster recovery planning and emergency access procedures via redundant voice servers and mobile products that allow for continuous dictation in the event of a server outage.

PowerScribe HIPAA Security Rule Compliance Features/Offering
Dictaphone, 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. Prior versions of PowerScribe software may not provide sufficient security features to adequately support the HIPAA Security Rule.
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

This datasheet provides details intended to assist an institution incompleting a HIPAA risk analysis of the PowerScribe® product.

Passwords can be administratively changed to revoke access in support of a sanction policy.

Various audit reports provide information vital to implementing the Information System Activity Review specification.

Dictaphone has a dedicated Manager of Information Security who is responsible for internal security policy.

Procedures can be provided which allow the remote access maintenance of the PowerScribe system to be controlled by the customer.

Passwords can be administratively changed to revoke access in support of termination procedures.

PowerScribe helps support the access authorization specification by providing the capability to implement centralized role based security through the use of groups that can be created based on roles, departments, geographic location or any other identifying criteria with each group and its accompanying users being granted unique rights and privileges.

Note: All versions of Encounters utilize user level authorization only.

PowerScribe provides a comprehensive capability to create and manage all 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:

■ **Author** – enables report authors access 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.

Note: See PowerScribe Admin Guide for privileges associated with roles.

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.

PowerScribe is certified to work with the following anti-virus packages:
■ Symantec Norton Antivirus ■ McAfee (known to work but not certified)

The Login Manager can be used to monitor all non-administrative users using the system. Inactive users can immediately be logged out. The following login statistics can be viewed at any time:

■ User ID – the user's 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.

Note: Remote and Last statistics are not available in the Encounters user interface.

The following password management features are available:
■ Masked password entry
■ Password aging and forced expiration
■ Administrative password reset and change
■ Settable minimum password length (v4.7) Not in PowerScribe Encounters product (v4.3)
■ Passwords encrypted in storage

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.

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:
- Veritas Backup Exec

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.

Contingency Plan
PowerScribe is compatible with backup and disk imaging products that are certified to work with the current Windows desktop and server operating systems.

Physical Safeguards

PowerScribe uses standard Windows workstations which support a variety of physical security mechanisms.

Dictaphone continually reviews customer requests for security features and enhancements based upon the results of internal risk assessment activities.
Dictaphone will execute HIPAA Business Associate agreements with its customers who purchase Maintenance, iChart or other services.

The PowerScribe system fully supports the creation, maintenance and use of unique user identifiers. The system can be configured to require an additional unique user identifier to sign a report.

Administrator accounts can be used to provide full access to system features in the event of an emergency.

PowerScribe has a configurable inactivity timeout feature that can be utilized to automatically logoff idle users within the application.

Third party encryption and decryption solutions can be used at the customer's discretion but are not supported by PowerScribe.

In addition to all standard audit and logging features of the Windows operating system and SQL server database system, PowerScribe includes a Report Manager feature that reports against tracked system activity across the PowerScribe system. Utilizing Report Manager, detailed transcription
reports can be generated based on the following data points:
- **Report#** – the report number
- **A** – a checkmark identifying an addendum
- **Visit#** – the visit number
- **Patient MRN** – the patient's medical Record Number
- **Patient Name** – the patient's name
- **DOB** – the patient's date of birth
- **Admin Time** – the date and time of the hospital visit
- **Doc Type** – the document type
- **Author** – the author of the report
- **Locked By** – the name of the person who has the report open for edits.
- **State** – the state of the report (Signed, Unsigned, Approved, Purg.)
- **Date/Time Dict.** – the date and time of the report dictation
- **Editor** – the user who edited the report
- **Signed By** – the user who signed the report

PowerScribe utilizes 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 at the administrative level and can be totally disabled.

PowerScribe is compatible with all Windows-based biometric and multi-factor authentication schemes when they are used as prescribed by the vendor.

PowerScribe relies upon lower level integrity and encryption services such as VPN, Windows operating system and TCP/IP networking devices for transmission security.

Giving
New Meaning
To Voice…

Dictaphone World Headquarters
3191 Broadbridge Avenue
Stratford, CT, USA
06614-2559
Tel: 1-888-350-4836
E-mail: healthcare@dictaphone.com
Web: www.dictaphone.com
Dictaphone Canada
2355 Skymark Avenue
Mississauga, Ontario, Canada
L4W 4Y6
Tel: 1-905-625-0300
Dictaphone Healthcare Solutions International
Commonwealth House
Chalk Hill Road, Hammersmith
London W6 8DW, United Kingdom
Tel: +44 (0)20 7878 5000
Dictaphone Healthcare Solutions Continental Europe
Dictaphone Europe AG
Ifangstrasse 91
8153 Rümlang
Switzerland
Tel: +41 (1) 817 76 76
Fax: +41 (1) 817 76 77

L-2912 Ver 1.0 6/05 *On Demand*