WHITE PAPER

Support for the HIPAA Security Rule RadWhere™ 3.0

NUANCE

SUMMARY

This white paper is intended to assist Nuance® customers who are evaluating the security aspects of the **RadWhere™ 3.0** 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 RadWhere 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 RadWhere 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 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. RadWhere 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 was required no later than April 21, 2005. Small health plans were required to 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 RadWhere 3.0 system was introduced to the market in August 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 5 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.

[1] Federal Register / Vol. 68, No. 34, pp 8336
[2] IBID
[3] Federal Register / Vol. 68, No. 34, pp 8343

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

RadWhere 3.0

- Dictation / Correction Client
- Administration Portal

The RadWhere 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.

RadWhere 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 the RadWhere system and developed this white paper. The paper describes HIPAA-related security features in the above mentioned version of RadWhere 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 RadWhere product features which will complement efforts to achieve HIPAA Security Rule compliance. The RadWhere 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	RadWhere Feature/Offering
Risk Analysis (R)	This white paper provides details intended to assist an institution in completing a HIPAA risk analysis of the RadWhere product.
Risk Management (R)	The RadWhere product includes a number of configurable security measures that improve an institution's ability to manage 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)	Two levels of authority, Administrator and System Administrator, are provided for administration the various security mechanisms featured in the RadWhere system.

Workforce Security

Standard and Specification	RadWhere Feature/Offering
Authorization and/ or Supervision (A), Workforce Clearance Procedures (A)	RadWhere's role-based user accounts 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 accounts can be administratively disabled or completely removed to revoke access in support of termination procedures.

Information Access Management

Standard and Specification	RadWhere Feature/Offering
Isolating Healthcare Clearinghouse Functions (R), Access Authorization (A)	RadWhere helps support the access authorization specifications by providing the capability to implement centralized role-based security through the use of user accounts that can be created based on roles, departments, geographic locations or other identifying criteria, such that users are granted unique user rights and privileges.
Access Establishment and Modification (A)	RadWhere helps support the access authorization specifications. RadWhere 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 user. • **Author** – enables report authors to the Dictation/Correction client to create reports. Includes roles for Attending, Resident, and Fellow. • **Transcriptionist** – enables access to the Dictation/Correction Client for editing and correction of dictated reports. • **Order Entry** – enables access to the Order Entry application to enter new patients and orders into RadWhere. • **Administrator** – enables access to perform administrator functions. • **System Administrator** – enables access to perform system administrator functions. • **Technologist** – enables access to create draft reports and set field values. • **Front Desk Staff** – enables access to scan patient documents. *Note: See RadWhere Administrator Guide for privileges associated with roles.*

Security and Awareness Training

Standard and Specification	RadWhere Feature/Offering
Security Reminders (A)	The RadWhere administration guide and periodic information articles sent to customers provide security related recommendations and instructions. The Nuance Professional Services Group 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.
Protection from Malicious Software (A)	RadWhere is certified to work with the following anti-virus packages: • Symantec™ Norton Antivirus™ • McAfee® (known to work but not certified)
Log-in Monitoring (A)	The Dashboard page in the administration portal can be used to monitor all users using the system. The following login statistics can be viewed at any time: • **Login ID** – the user's Login ID • **Name** – the user's name • **Session length** – duration the user has been logged in • **Workstation** – the name of the user's client machine • **Report info** – information about the report the user is currently working on • **Last action** – the last workflow action by the user. The Account Audit page in the administration portal can be used to view a history of events related to a user's account, including logon, logoff, and password.
Password Management (A)	The following password management features are available: • Masked password entry • Password aging and forced expiration • Administrative password reset and change • Strong password option requiring minimum length of 6 characters with at least one letter and one digit • Password encrypted in storage

Security Incident Response

Standard and Specification	RadWhere Feature/Offering
Response and Reporting (R)	The RadWhere exam explorer and 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	RadWhere Feature/Offering
Data Backup Plan (R)	Backups of critical RadWhere files can be made with any software which can successfully handle SQL Server databases and Windowss. RadWhere has been tested with the following backup product: • Veritas Backup Exec
Disaster Recovery Plan (R)	Disaster Recovery procedures for RadWhere can be crafted which are based upon standard Windows and SQL Server disaster recovery technologies, strategies and third party solutions.
Emergency Mode Operations Plan (R) **Testing and Revision Procedures (A)** **Application Data Criticality Analysis (A)**	RadWhere is compatible with backup and disk imaging products that are certified to work with the current Windows desktop and server operating systems.

Evaluation

Standard and Specification	RadWhere Feature/Offering
Response and Reporting (R)	Nuance continually reviews 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	RadWhere Feature/Offering
Written Contract or Other (R)	Nuance will execute HIPAA Business Associate Agreements with its customers who purchase Maintenance, or other services.

PHYSICAL SAFEGUARDS

Physical Access Controls

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

Workstation Use (R)

N/A

Workstation Security (R)

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

Device and Media Controls

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

TECHNICAL SAFEGUARDS

Access Controls

Standard and Specification	RadWhere Feature/Offering
Unique User Identification (R)	The RadWhere system fully supports the creation, maintenance and use of unique user identifiers. RadWhere also supports standard Lightweight Directory Access Protocol (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)	RadWhere 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 RadWhere.
Audit Controls (R)	In addition to the standard audit and logging features found in a Windows operating system and SQL server database system, RadWhere includes a robust auditing feature that records activities performed by administrators and users of the RadWhere system. Database tables capture detailed information concerning the activities performed in each of the RadWhere application areas — Administrator (ADM), RadWhere API (API), Dictation/ Correction (DC), Order Entry (OE), and System (SYS). The following information is captured for every event: • Date and time • Computer name • Application area • User name • Admin user name • Description of event Other activities recorded include: • User logins and logouts • Password changes • Add, modify, delete users • Preference changes • Order information created or updated by RIS • Reports created, edited, or deleted • Reports signed • Reports faxed

Integrity

Standard and Specification	RadWhere Feature/Offering
Mechanisms to Authenticate ePHI (A)	RadWhere 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. Configurable workflow processes can be implemented to facilitate integrity checking by requiring transcribed reports to be reviewed for accuracy prior to being signed.
Person or Entity Authentication (R)	RadWhere is compatible with all Windows-based biometric and multi-factor authentication schemes when they are used as pre-scribed by the vendor. RadWhere supports Lightweight Directory Access Protocol (LDAP) for those institutions that leverage LDAP services to authenticate users.

Transmission

Standard and Specification	RadWhere Feature/Offering
Integrity Control (A) Encryption (A)	The RadWhere Web portal supports Secure Sockets Layer (SSL) communication between browser-based clients and servers to protect data integrity and data confidentiality. The RadWhere Windows client connects to the database without encryption, and therefore relies upon lower level integrity and encryption services such as VPN, Windows operating system and TCP/IP network devices for transmission.

L-3302 7.10 PF

The experience speaks for itself™

NUANCE COMMUNICATIONS, INC.
ONE WAYSIDE ROAD
BURLINGTON, MA 01803
800 350 4836
NUANCE.COM/HEALTHCARE

NUANCE