

Support for the HIPAA Security Rule

GoMD Dictate[®] System

Summary

This whitepaper is intended to assist Dictaphone customers who are evaluating the security aspects of the GoMD Dictate® system as part of their risk analysis required for Health Insurance Portability and Accountability Act (HIPAA) Security Rule compliance. The paper describes specific features of the GoMD® 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 GoMD 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. GoMD 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 ensure that any individual healthcare provider meets its HIPAA compliance obligations.

GoMD™ Overview

Dictaphone's GoMD system was introduced to the market in 2002 as a mobile dictation and documentation solution that allows healthcare providers to create and manage medical reports at the point of care using the HP iPAQ® handheld device to dictate patient reports and send them to the Central System for speech recognition or manual transcription. The GoMD suite of applications is designed to leverage existing investments in Dictaphone's Enterprise Express® speech recognition solution while combining secure mobility and wireless technology to dictate reports, review active patient list, electronically sign reports and accurately capture changes anywhere and anytime.

The paper provides a brief analysis of how GoMD supports an organization's efforts to comply with HIPAA's Security Rule standards. The datasheet describes HIPAA-related security features in the latest version of software and includes the following product components: ■ GoMD Dictate – version 3.0

The GoMD, system as a peripheral extension of Enterprise Express, augments and leverages its multiple levels of system security to protect patient confidentiality and user or group privileges that grant or restrict access to specific product features. Via Enterprise Express v6.5, the system is equipped with comprehensive audit and reporting capabilities to provide details related to documentation creation, users, editors, signers, timestamps, viewing, distribution, etc. Enterprise Express provides dictation redundancy software and hardware configurations that support disaster recovery planning and emergency access procedures using redundant voice servers, allowing continuous dictation for the GoMD product in the event of a server outage.

Note: Many PDA devices are shipped "wireless-ready" and support communication options such as infrared beaming, Bluetooth, WLAN and wireless WAN. Dictaphone recommends that only safe, authorized communication mechanisms are used. Organizations should establish controls that define when, where and how and employee can communicate when using a mobile device.

GoMD 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 GoMD system and developed this white paper. The paper describes HIPAA-related security features in the above mentioned version of GoMD software; however, it does not discuss security features in previously released versions. Prior versions of GoMD 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 GoMD product features which will complement efforts to achieve HIPAA Security Rule compliance. The GoMD 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

Standard and Specification

Dictaphone Features/Offering

Security Management Process

Risk Analysis (R)

Risk Management (R)

Sanction Policy (R)

Information System Activity Review (R)

This datasheet provides details intended to assist an institution in completing a HIPAA risk analysis of the GoMD® product.

Passwords for the GoMD Dictate application can be administratively changed to revoke access in support of a sanction policy. In version 4.0, fully centralized administration of user credentials, security controls and access granting will further support sanction policy enforcement.

Various Enterprise Express® audit reports provide information vital to implementing the Information System Activity Review specification against the GoMD peripheral.

Assigned Security Responsibility (R)

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

Workforce Security

Authorization and/or Supervision (A)

Workforce Clearance Procedures (A)

Termination Procedures (A)

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

N/A

Passwords for the GoMD Dictate application can be administratively changed to revoke access in support of termination procedures. Third party solutions supplied by HP on the iPAQ for centrally managing iPAQ device security do not conflict with GoMD operations when used as prescribed by HP.

Information Access Management

Isolating Healthcare Clearinghouse Function(R)

Access Authorization (A)

Access Establishment and Modification (A)

GoMD 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; each group and its accompanying users can be granted unique rights and privileges via Enterprise Express.

GoMD utilizes Enterprise Express's comprehensive capability to report user rights and access privileges granted to GoMD Dictate application users via the Explorer application.

Security Awareness and Training

Security Reminders (A)

The GoMD 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.

Administrative Safeguards *continued*

Standard and Specification

Dictaphone Features/Offering

Security Awareness and Training

Continued

Protection from Malicious Software (A)

N/A

Log-in Monitoring (A)

All login and logoff activity for GoMD can be logged and reported using the Access Audit feature of Enterprise Express. Accounts can be set to lock after multiple failed login attempts, thus requiring administrative intervention to re-enable the account with a configurable lockout duration.

Password Management (A)

The following password management features are available for the GoMD Dictate application via the Enterprise Express password management features:

- Masked password entry
- Settable minimum password length
- Password aging and forced expiration
- Administrative password reset and change
- Alphanumeric password complexity
- Configurable failed login attempt lockout
- Configurable lockout duration
- Explicit login failure message

Security Incident Procedures

Response and Reporting (R)

Enterprise Express Access Audit logging data can be utilized in responding to incidents involving GoMD in support of the forensics and investigation processes. Access Audit logging data can be exported to CSV or comma delimited formats for additional processing via third party products. Dictaphone supports the use of third party monitoring and notification programs which detect and track the activity on iPAQ Pocket PC mobile devices.

Contingency Plan

Data Backup Plan (R)

Backing up the GoMD web server should be an extension of the existing Enterprise Express server backup procedures. Enterprise Express has been tested with the following backup product: ■ Veritas Backup Exec

The iPAQ device should regularly be backed up using HP provided Backup tools or Microsoft ActiveSync. iPAQ Backup backs up to a memory card or iPAQ File Store folder. The data is retained should the battery discharge completely or a full reset of the iPAQ be performed. ActiveSync can be utilized to selectively backup certain folders or the entire device to the docking workstation.

Disaster Recovery Plan (R)

Disaster Recovery procedures for GoMD would be an addendum to those created for the Enterprise Express system, which are based upon standard Windows, IIS, SQL Server disaster recovery technologies, strategies and third party solutions. Dictaphone supports a customer supplied clustered web server architecture or cold standby servers for the GoMD web server.

Emergency Mode Operations Plan (R)

In the absence of a dictation or web server, GoMD can be used for dictation and subsequent uploading of reports once the server becomes available.

Testing and Revision Procedure (A)

*Application and
Data Criticality Analysis (A)*

Administrative Safeguards *continued*

Standard and Specification

Dictaphone Features/Offering

Evaluation

Response and Reporting (R)

Dictaphone continually reviews customer requests for security features and enhancements based upon the results of internal risk assessment activities.

Business Associate Contract and Other Arrangements

Written Contract or Other Arrangements (R)

Dictaphone will execute HIPAA Business Associate agreements with its customers who purchase Maintenance, iChart or other services.

Physical Safeguards

Facility Access Controls

Contingency Operations (A)
Facility Security Plan (A)
Access Control and Validation Procedures (A)
Maintenance Records (A)

N/A

Workstation Use (R)

N/A

Workstation Security (R)

GoMD Dictate uses standard Windows workstations and iPAQ handheld Pocket PCs which support a variety of physical security mechanisms.

Device and Media Controls

Disposal (R)
Media Reuse (R)
Accountability (A)
Data Backup and Storage (A)

Dictaphone recommends that customers implement strict asset management controls, strong power-on passwords and inactivity timeouts for all iPAQs storing ePHI. Sensitive GoMD data can be stored on the SD card with data files encrypted and voice files only replayable via the GoMD Dictate application. Physical access control mechanisms provided by HP on the iPAQ do not interfere with GoMD operations when used as prescribed by the vendor.

Technical Safeguards

Access Control

Unique User Identification (R)

The GoMD Dictate application 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.

Note: Customers must enable the iPAQ power-on password and configure it to utilize strong passwords at the device level.

Technical Safeguards *continued*

Standard and Specification

Dictaphone Features/Offering

Access Control

Continued

Emergency Access Procedures (R)

Administrator accounts can be used to provide full access to voice and text files that have been synchronized to the GoMD Dictate application or wirelessly to the GoMD Central System server in the event of an emergency.

Automatic Logoff (A)

GoMD Dictate has a configurable inactivity timeout feature that can be utilized to automatically logoff idle users within the application. An inactivity timeout can also be set on the iPAQ which would lock the device should the specified inactivity timeline be reached.

Encryption and Decryption (A)

Dictation data files are encrypted on the iPAQ and recorded voice files can only be replayed via the GoMD Dictate application. Third party encryption and decryption solutions are not supported by GoMD.

Audit Controls (R)

In addition to all standard audit and logging features of the Windows operating system, IIS and SQL server database system, Enterprise Express includes an Access Audit feature that can track system activity across the Enterprise Express system of which GoMD is a peripheral. The Access Audit feature runs under Job Lister and allows reporting on Enterprise Express system events.

The following elements are logged for future reporting: Username, Computer Name, System, Patient ID, Document ID, Job ID, Date, Access Type create, view, listen, etc. and Logon/Logoff. Logged activity data may be exported to a CSV file for further analysis and archiving.

Integrity

Mechanism to Authenticate ePHI (A)

GoMD utilizes application, operating system and device 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.

Person or Entity Authentication (R)

The HP iPAQ supports strong complex passwords to authenticate a person to the device. GoMD Dictate utilizes one factor authentication comprising of a unique user ID in conjunction with a password to authenticate a person or entity to the application. Additional passwords are used for various available services such as electronic signing. Biometric or two-factor authentication mechanisms provided by HP on the iPAQ do not conflict with GoMD operations when used as prescribed by HP.

Transmission

Integrity Controls (A)

Encryption (A)

iPAQ devices support PEAP which encrypts all authentication data passed over the 802.11b wireless network. GoMD recommends and supports lower level integrity and encryption services such as a VPN for complete wireless transmission security.

