

## DVI/VXP Security Alert Regarding HITECH Act Changes to HIPAA

### Overview

This notice is intended for all distributors, dealers and end-users of Digital Voice, Inc. (DVI) and Lanier/MedQuist VXP software and Fusion software version 8.0 software components designed for use with both the DVI and VXP digital dictation systems. Although these products are no longer marketed, there exists a substantial installation base of DVI dictation systems and VXP dictation systems still in use in healthcare facilities and all are at risk under the new HITECH Act provisions.

On April 17, 2009, the U.S. Department of Health and Human Services (HHS) issued proposed information security guidance, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act passed as part of American Recovery and Reinvestment Act of 2009 on February 17, 2009. The HITECH Act requires covered entities and business associates, as well as others, to provide notice of information security breaches affecting “unsecured protected health information”. The HITECH Act further requires the Secretary of HHS to specify technologies and methodologies that would render protected health information (PHI) unusable, unreadable, or indecipherable to unauthorized individuals. If covered entities, business associates and vendors of personal health records apply the technologies and methodologies specified in the guidance to protected health information, they will not be required to provide notice to affected individuals, HHS or the media, as otherwise required by the HITECH Act, in the event the information is breached.

Upon review of the current definitions available, the security features of the DVI dictation systems, VXP dictation systems and Fusion Version 8.0 for DVI/VXP do not provide the technology necessary to adequately protect dictation and dictation data to meet the definition to secured protected health information data.

### Risk Assessment

The following represents a first-pass evaluation of these software applications and other, not yet known, areas of risk may be unidentified or later identified. Further review with future notice may disclose other deficiencies to meet the standard to secure patient health information.

#### *Encryption:*

Encryption is the process of using algorithmic schemes to alter data to make it indiscernible to those who should not have access to the data. Specific encryption methods use *keys* for those individuals and applications that need to restore the data back to a usable state. The identified systems do not deploy encryption.

1. Data stored on the server is not stored by the application in an encrypted format. In many cases, dictation files containing PHI, are simply stored as .WAV files that are easily opened and played using free software from MS/Windows and many other media applications.
2. If dictation or transcription client/server application such as VoiceWave Player, VXP Player, VoiceWave Dictate and VXP Dictate are utilized, these applications do store data on the local client PC unencrypted. This data is potentially stored as a .WAV file.

3. The dictation and transcription client/server applications identified allow for the end user to select to archive dictations locally. If this feature has been activated, personal computer workstations in and outside a firewall may house these unencrypted .WAV files.
4. The transmission of dictation data to and from the client applications and the server applications do not employ encryption during transport. All of these applications allow for transmission over the public Internet, a practice that is widely utilized for remote dictation and home-based or remote transcription.

#### *Authentication:*

Application authentication, or the process of resolving a user login to an application, sends user names and passwords to and from the server applications over a network or Internet connection. Proper security provisions require the periodic change of passwords with defined intervals as well as communicating this login information between client application and server in a secure manner.

1. The security provisions do not provide for the deployment of any password change management.
2. Login information as passed from client to server and server to client is not encrypted.

#### *Auditing*

Auditing or presenting reports for disclosure is essential to report who and when PHI was accessed. Logs or reports, easily generated, are required to provide this information to CMS or upon a patient request.

1. The identified systems do not provide complete audit trails of accesses by users and by dictation.
2. The limited access logs available store the information for just 90-days and then are automatically purged.

This memo is a basic summary of the risks associated in using the identified systems under the new HITECH provisions of HIPAA. A complete risk assessment is available upon request and action is encouraged. Please contact Dolbey or your support organization for a complete risk assessment and an action plan for compliance. Reach an application specialist at 800-878-7828 for further details.