HIPAA Privacy Statement

Our Company works with industry groups to ensure that its products and services meet or exceed industry standards with respect to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Our Company’s products and services are specifically designed to include features that help our customers comply with HIPAA. Our Company uses a relational database that employs a secure login process requiring a user name and password.

Our Company supports role-based access. That is, users are assigned to groups, each with certain access rights, which may include the ability to edit and add data or may limit access to data. When a user adds or modifies data within the database, a record is made that includes which data were changed, the user ID, and the date and time the changes were made. This establishes an audit trail that can be examined by authorized system administrators.

Products

Our Company’s products incorporate the standard codes required by the HIPAA transaction standards for use in Audiology and Hearing Aid Dispensing, including the related subsets of the International Classification of Diseases, 9th Edition, Clinical Modification (ICD9-CM) and Current Procedural Terminology, 4th Edition (CPT-4).

Our Company utilizes a relational database that ensures all access is through a secure login process requiring a user name and password. Our Company supports role-based access. Within Our Company, users are assigned to groups and these groups in turn are assigned access rights, which may include the ability to edit and add data or may limit access to data. When a user adds or modifies data within the database, a record is made of what data was changed, the user and the time at which the data was changed establishing an audit trail that can be examined by authorized system administrators.

Customer Support

Our Company’s product support staff will work with customers to help implement Our Company’s products in a HIPAA compliant environment. All remote access to customer patient information by Our Company product support staff will be made using a fully encrypted protocol.

Business Associate

HIPAA requires health care providers to enter into “business associate” contracts with certain businesses to which they disclose patient health information. These business associate contracts generally require the recipients of such information to use appropriate safeguards to protect the patient health information they receive. To perform certain service and support functions, Our Company personnel may need access to patient health information maintained by its customers. As a result, Our Company may be considered a “business associate” of customers to whom it provides such services. Our Company will be providing its customers with a new standard business associate agreement that complies with HIPAA requirements. Our Company’s new business associate contract will generally assure its customers that the company will use patient information obtained from them to provide services and support only and will safeguard that information from misuse. The agreement will be effective on March 15, 2012 the current compliance date for the HIPAA privacy regulations, or any later adopted compliance date.

Privacy & Security Policy

To implement these business associate requirements and protect the confidentiality and integrity of the patient information it receives, Our Company’s Privacy and Security Policy will:

- Provide that the company obtain and use confidential patient health information obtained from its customers only as necessary to perform customer service and support functions;

- Limit access to such information to those employees and agents who perform identified service and support functions;
- Prohibit disclosure of patient health information received from customers to persons who are not employees or agents of the company in the absence of express approval from the legal department and, if appropriate, the customer and/or patient;
- Require all employees and agents of the company to report uses and disclosures of patient information that are not permitted by Our Company's Privacy and Security Policy;
- Provide that Our Company investigate all reports that patient health information was used in a manner not permitted by its Privacy and Security Policy and will impose appropriate sanctions for conduct prohibited by the policy;
- Establish that Our Company employees who may come in contact with patient health information receive training regarding Our Company's Privacy and Security Policy and the importance of protecting the privacy and security of patient health information; and
- Provide for the storage and transmission of patient health information received from customers in a secure manner that protects the integrity, confidentiality and availability of the information.