HEALTHY TEEN SCREENER SYSTEM HIPAA COMPLIANCE INFORMATION

The Healthy Teen Screener System has been designed from the ground-up in full compliance with current applicable HIPAA guidelines and regulations. The Screener includes a secure online database, a password-protected web site, a secure Palm PDA data conduit and a client side Palm screener application. Each layer of each component of the system is protected by industry-standard health information technology measures to maintain the privacy and security of patient information. Identifiable patient information entered and stored in the system is limited. The Palm Screener application and the secure online database do not store patient names, only initials of the first and last names. In addition, the database stores age, grade in school, gender, and (optionally), local medical record number. All of these parameters are encrypted using industry-strength algorithms both in the PDA client database and in the secure online database and remain encrypted all the time whether they are stored or transmitted between the PDA client and the online database. Other data elements include non-identifiable health information.

PDA CLIENT

The PDA Screener client is a Palm Operating System application. The application is password-protected at multiple layers. Access to the application is granted only after proper credentials are entered (user authorization). The Palm application resides on a particular PDA unit with a unique name. This unique name is stored and tracked with each patient record (user identification). When a patient record is saved at the end of a session, all identifiable data is encrypted and stored temporarily on the Palm device for secure transmission. In addition, access to patient records and authorization for running reports within the application is granted only upon successful password authentication.

PDA CONDUIT

The PDA data conduit opens a secure connection to the online Screener database after successful authentication and identification utilizing standard database protocols for SQL client connections. In the course of a unidirectional synchronization process, encrypted data is transmitted from the PDA directly to the online database and the PDA client is then disconnected and the database connection is closed.

ONLINE DATABASE

The secure online screener database is a dedicated and commercially hosted Microsoft SQL database. Access to the database is restricted to authorized clients and the database administrator. Authorized clients have limited and role-based access privileges that exclude

database management/administrative functions and access to records other than their own. Only the database administrator has unrestricted access to the database. However, individual patient records cannot be identified in the course of administrative procedures and they remain encrypted. Regular backups of the online database are performed by the administrator and encrypted backup files are stored at a separate secure location.

SCREENER WEB INTERFACE

Health Screener web clients can review and manage their own records via a secure web interface. The dedicated secure web site is hosted commercially in the same environment. The presentation layer utilizes standard Microsoft ASP technology. Client connections are established via 128-bit encrypted Secure Socket Layer (SSL) based sessions to prevent session hijacking and man-in-the-middle attacks. Access to the web interface is granted only upon authorization and identification via a proper username/password combination specific to each screener user. Once signed in, user actions are logged and database operations are traceable based on date/time and user ID. Sessions expire in a specific time to prevent unauthorized users from joining an established session on a client computer.