HEALTHMASTER HOLDINGS LLC

DATA SECURITY AND PRIVACY PLAN

(New York)

1. **Services Provided**:

Healthmaster Holdings LLC ("Healthmaster") develops and markets the HealthOffice® Anywhere suite of electronic health records and case management services for nursing, mental and behavioral health and special education, Medicaid billing integration and a parent portal ("HealthOffice Anywhere") to public school districts and private schools (collectively the "Districts"). The parent portal (the "Portal") is a connection through which the District can securely communicate health related issues directly to parents. HealthOffice Anywhere operates in a web-based Software as a Service model. No software is physically provided and no HealthOffice Anywhere data is stored within the District's computer system. District personnel access HealthOffice Anywhere through an internet based secure connection.

Each District using HealthOffice has a separate Database in which their student health records are stored. HealthOffice collects student personally identifiable information ("PII"): (i) electronically from the District's student information system; (ii) inputs from direct service providers, supervisors and administrators; (iii) electronically from state authorities or health insurers with specific consent from parents. This Data Security and Privacy Statement explains the basis for obtaining the PII, the manner in which it is securely transmitted and stored and the privacy protection afforded the PII. Healthmaster policies are in compliance with the Family Educational Rights and Privacy Act ("FERPA"), the Education of All Handicapped Children Act ("EHA") and the Health Insurance Portability and Accountability Act ("HIPPA"). Healthmaster continuously monitors changes in state and federal law relating to student privacy and data security and will incorporate.

2. **Authorization to Collect PII**.

Districts must agree to Healthmaster's HealthOffice Anywhere Master Web Services Agreement ("Web Services Agreement"). Through the Web Services Agreement, Healthmaster is designated a "school official" with "legitimate educational interests" (as those terms are defined under FERPA) to collect and store PII for purposes of providing the HealthOffice Anywhere suite of electronic health records software to the District. Specifically, (1) the collection of PII and student health data within HealthOffice Anywhere are services and functions for which the District would otherwise use its own employees; (2) Healthmaster is under the District's direct control with respect to Healthmaster's access to and use of PII; and (3) Healthmaster is subject to the requirements of federal and state law with respect to Healthmaster's access to and use of PII. With respect to billing Medicaid (through state government or state-contracted health insurance companies), Healthmaster is authorized both by parental consent and a Medicaid Billing/Clearinghouse Agreement with the District to transmit PII for the sole purpose of billing for direct services rendered to a student

3. **Data Security**.

HealthOffice Anywhere contains layers of security protection to ensure the integrity and safety of student PII.

A. User Security: Each user from a District is assigned a unique identifier and password. The District also assigns permissions for each user. For example, a direct service provider can be restricted to view and input data only for her or his case load. A supervisor will generally have rights to see the records of her or his subordinates and an administrator may have rights to the entire database. When a user logs into HealthOffice Anywhere for the first time and also when changing passwords, the user acknowledges his or her eSignature and that entries made into HealthOffice Anywhere constitute an affirmation of the validity and accuracy of the entry as if signed by hand.

HealthOffice Anywhere maintains both access logs and audit logs. The access log tracks each successful and unsuccessful attempt to access a student record. The audit log maintains a record of each entry made by user, date and time. No entry can be deleted. Both logs provide the District with real time data to monitor access and integrity of the data. In addition, HealthOffice Anywhere has an automatic time out feature to prevent data screens from remaining open for protracted periods of time.

B. Data Transmission Security: Login data and all transmission of data to and from the District are encrypted through the highest level of SSL encryption. All security related data is encrypted to provide maximum user security and to meet all electronic signature requirements.

C. Physical and Electronic Security: All of the student information in HealthOffice Anywhere Databases are stored in an off-site, third-party data center in Michigan on servers and equipment used only by Healthmaster. Data center access to those servers and equipment is limited to certain Healthmaster employees and Data Center technicians. Biometric scanning is required for data center access. The data center is monitored by security staff and security cameras on a 24x7 basis. The data center is an unmarked facility to maintain a low profile and physical security is audited annually by an outside firm. The data center has multiple backup and power systems to allow for anytime online access without loss of data.

System and data backups are automatically performed daily with full reporting. Custody of the backup data is maintained by Healthmaster Data Center staff. Backups are managed for eight (8) days and expired data is destroyed. Deleted data and other information is wiped per DOD 5220.22-M data sanitation criteria.

The Database for each District is maintained in separate silos so that users from one District have no ability to access data from another District. Healthmaster uses a security hardened patched

operating system. System patching has been configured by the data center to provide ongoing protection from exploits. Healthmaster servers have dedicated firewall and VPN services to help block unauthorized system access with dedicated intrusion detection devices to provide an additional layer of protection against unauthorized system access. Healthmaster does not print any information at the data center.

The data center provides a continual risk assessment and security consultation. The data center electronic security measures are audited annually by an outside firm to confirm best practices are being utilized. Those reports are available to the IT staff of our customers.

D. Healthmaster Personnel and Security: Healthmaster has strict written policies about data handling within its organization with an emphasis on security. Only a few Healthmaster employees, selected based upon their responsibilities to maintain and manage customers' databases, are granted limited rights of access to PII solely to perform their job functions. Support personnel (who cannot access a District's database) may also be exposed to PII in connection with generating custom reports or responding to user questions seeking assistance with the input or output of PII into/out of HealthOffice Anywhere. Paper records generated during the support of a customer are destroyed via Level 3 DIN 32757-1 standard. All Healthmaster support personnel must agree, in writing, to maintain the confidentiality of student PII and are trained in their statutory and contractual obligations of confidentiality.

E. Notification of Breach of Security: In the event of a security breach and unauthorized disclosure of PII, Healthmaster shall provide notification as soon as practicable and shall at all times act in accordance with its obligations under the relevant federal and state law and the Web Services Agreement.

4. **Privacy of PII**.

A. Student Privacy Pledge: Healthmaster has signed the Student Privacy Pledge (www.studentprivacypledge.org/privacy-pledge/), in which vendors of school services pledge to carry out responsible stewardship and appropriate use of student personal information. Under the Student Privacy Pledge, Healthmaster has agreed, in part, to: (i) not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student; (ii) not sell student personal information; (iii) not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students. Further, all documents used by Healthmaster that are directed to parents disclose clearly and in a manner easy for parents to understand, what types of student personal information is collected and the purposes for which the information is used or shared with third parties.

B. Uses of PII: Healthmaster uses PII only in connection with creating, maintaining and storing student health records in accordance with the Web Services Agreement as might be modified by the parties to that agreement. If the District is using the Parent Portal, the Portal permits the transfer of PII between the District and parents in a secure manner and the District must enter

that data into HealthOffice Anywhere; Healthmaster personnel are not part of that process. If Healthmaster has been granted authority by the District and the parent/student to bill Medicaid or third-party insurance companies for school based services, Healthmaster may use a student's PII for those purposes. All billing services are performed in accordance with a Medicaid Billing/Clearinghouse Agreement between Healthmaster and the District, and the agreement may also provide authorization for Healthmaster to use a vendor for insurance billing purposes. The confidentiality and privacy of a student's PII in the billing process will be in strict compliance with HIPPA and any vendor used by Healthmaster will also be required to comply with the same or stronger security and privacy obligations observed by Healthmaster.

C. Limitations on the Use of PII: The District owns all of the PII which has been put into or stored within HealthOffice Anywhere and the District controls the use and dissemination of such data. Healthmaster does not sell PII or any information derived from PII such as aggregated and deidentified student health information. Healthmaster does not use PII or any information derived from PII to advertise (targeted or otherwise) goods or services to users of HealthOffice Anywhere.

D. Compelled Disclosure of PII: If Healthmaster is compelled by law to disclose PII, it shall provide the District and/or any other contracted party with prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, if the District and/or any other contracting party is able and wishes to contest the disclosure. Healthmaster will also comply with any other notice requirement required by law as it relates PII.

E. Correction of Erroneous PII: Healthmaster is aware of and supports a parent's right under federal and many state laws to correct information in a student record that is erroneous. Healthmaster does not directly access a student's health record to input or correct data; therefore, only the District has the ability and access to correct any PII stored in HealthOffice Anywhere. With the approval of the District, Healthmaster will support the correction of any erroneous PII.

F. Return/Destruction of PII: Upon written request by the District made within 45 days of the effective date of termination, Healthmaster will make available a onetime download of the District's database as a Microsoft SQL Server database backup (.bak) as it then exits. Any additional downloads of data will be at Healthmaster's then current charge for such service. After termination Healthmaster shall, unless legally prohibited, permanently delete all of the District's PII and the database in its systems or otherwise in Healthmaster's possession or under its control.