ELECTRONIC DATA MANAGEMENT

POLICY

Metro Support Services, Inc. uses an electronic data management system (Therap) for documentation and file management. Therap is a web-based service that provides for documentation and communication needs of Metro Support Services, Inc. providing support to people with developmental disabilities. It offers an easy and efficient alternative to the immense amount of paper work that is currently done by hand.

In order to comply with CMS Electronic Signature Guidance, Health Insurance Portability & Accountability Act of 1996 (HIPAA), Uniform Electronic Transactions Act (UETA) and E-SIGN (The Electronic Signatures in Global and National Commerce Act), compliance guidelines and requirements for the use and storage of electronic data records, Metro Support Service's electronic data records will be made available via a special access account for review and will be retrievable for authorized state survey team members, auditors and investigative employees. All modules will be made available for review, including activity tracking, secure communications, archive data, management reports, GER (Incident Reports), behavior data, eMAR, personal finance, IP and ISP Data and health tracking, billing information, staff training records, T-Log notes, and periodic reports, etc.

Staff Training

Metro Support Services, Inc. provides employees training in the use of Therap, methods and requirements for documentation, the use of searches, and summary data and reports for all modules. Online training, "walkabouts", automated training, webinars, a User Guide, online help, feedback, and FAQs are available for all users on: www.TherapServices.net.

Metro Support Services, Inc. employees and Independent Contractors will receive training in the following procedures:

- Clients' protected health information (PHI) should always be communicated securely, e.g., using secure HTTPS, a cryptographically secured protocol and interfaces
- Employees and Independent Contractors will be instructed in the authorized use of PHI for clients in their care, and to not discuss confidential information outside of their place of employment
- Employees and Independent Contractors will proceed with caution when saving electronic files containing PHI or files exported from THERAP to Excel or PDF
- Employees and Independent Contractors should not share their personal login information with others, write down their login information on paper, or save them in electronic files that can be accessed by others.

- While accessing the system from a shared computer or a public place, employees and Independent Contractors should not leave the computer screen unattended, delete all information from those computers, including clearing caches, cookies and temporary files.
- Metro Support Services, Inc. employees and Independent Contractors are advised not to store data on personal computers, laptops, or other storage devices, and any files containing PHI should be deleted after the work has been completed. This however will not apply to documents scanned into Therap by employees as Metro Support Services, Inc. maintains all client information / data in agency.
- Management reports, behavior Information, nursing, summary reports and other reports containing PHI may be printed or copied for use as required for Metro Support Services, Inc. business, per Metro Support Services, Inc.policy, or as required by state or federal regulation

Therap Administrators

Metro Support Service's Therap Administrators will be trained by Therap employees in the use and management of electronic data within the secure database. These selected Administrators are responsible for proper assignment of access privileges to users, setting up password policies, and activating/deactivating user accounts. Administrators will be required to have a clear understanding and sound knowledge of the various application capabilities and the underlying HIPAA regulations and E-sign policy, including:

- **Access Control:** Administrators are responsible for assigning proper roles and privileges to users to grant them access to systems while at the same time restricting access only to authorized information. Administrators are also responsible for updating these user access privileges assigned in accordance with changing job responsibilities and authority.

- **Implement Password Policy:** Administrators are able to set up and implement a suitable password policy for Metro Support Services, Inc.by specifying specific properties, including the minimum length, number of letters, digits, special characters required, and the policy regarding the password expiration periods. Metro Support Services, Inc. will not record, or inquire regarding employees' or Independent Contractors' passwords, or assign passwords to employees or Independent Contractors. Metro Support Services, Inc. may reset a temporary password at the request of employees or Independent Contractors who have been locked out of the system, however, employees and Independent Contractors will be asked to reset their temporary Therap System password immediately.

- **Managing User Accounts:** Administrators are responsible for creating and activating Therap accounts for employees and Independent Contractors and providing them with the required login information. Administrators will instruct new account holders to create passwords. If users forget their passwords, login names or provider codes, they will ask their Administrators for this information. (Therap Customer Support will not alter or supply users' login information, except for agency Provider Administrators.). Administrators may also disable employees' or Independent Contractors' user accounts when they terminate employment or contract, are on Administrative Leaves, or extended leaves.

- **Electronic Signatures:** Each employee or Independent Contractor shall choose a password of their choice to enable access to the system and to review activity tracking. The electronic signature tracks time and date stamps of all your entries within Therap. Employees and Independent Contractors shall NEVER give this password to any other employees or Independent Contractors. Violation of this policy may result in immediate disciplinary action.

- **Assignment of Roles and Caseloads:** Therap implements a multilevel access mechanism based on roles and clients. Metro Support Services, Inc.can specify the level of access available to particular users of the systems and grant permission accordingly. Administrators will assign users a specific list of roles for access privileges, as well as access to a specific caseload(s) of clients based upon their need to know, access, and level of responsibility.

- **Tracking User Activities:** **A**dministrators are able to track users' activities by using the Therap Activity Tracking module. The module is equipped with the capability to record and report on activities of all user accounts. The Activity Tracker will record all users accessing the system, including, time, date, login name, user name, IP address, and all activities, including viewing of information, creation or modification of any and all data or records. Administrators with this role or option can detect any attempts to breach the system security (failed login attempts) or other misuse. The Therap system is monitored by security systems and Therap employees for unusual activity. As needed, Therap services will provide training and support materials for Administrators to learn about these and other HIPAA compliant Therap features.

Message Integrity

All communications between end users' browsers and the Therap application are carried over HTTPS, a cryptographically secured protocol. No third parties can modify the data transferred or modify the data stored in Therap without going through the application. The data is stored in multiple secured locations, guaranteeing its safety from natural and manmade disasters.

- **Secure Sockets Layer (SSL)**: SSL is the international standard used to ensure protection of data during transmission over the internet. SSL provides endpoint authentication and communications privacy over the Internet using cryptography. The protocols allow client/server applications to communicate in a way which is designed to prevent eavesdropping, tampering and message forgery. Called communications from users to the Therap system use SSL, and thus are secure during transmissions.

- **Non Repudiation:** As data is stored securely no users can access the data without proper privilege and audit trail (activity tracking), and no users can deny the association of their identity with documents stored in Therap. *Initial*__________
- **User Authentication:** All users, including Therap employees, must authenticate with a unique login name and a secret password to gain access to the system.

- **Session Expiration:** Therap has a session expiration mechanism such that a session expires when a user has not used the system (i.e., has not hit any key on the keyboard or clicked on a button on the form) for half an hour. The system displays a countdown message for 5 minutes before the session actually expires. If users want to resume work, they can cancel the expiration by simply clicking a button on the countdown message. This is a security feature which prevents unauthorized personnel from using their login in cases where users may have left the program without logging out.

- **Altering over Non-Secure Media:** The Therap system assures that no PHI is transmitted over media, including email, text messaging, paging, while still providing a flexible alerting mechanism. For example, users may configure their notification properties to receive email or text messages that would let them know about critical incident reports being filed without revealing any PHI. When secure media, such as SComm and FirstPage, are used for alerting, the system allows PHI, such as clients' names to be included.

- **Secure Communications:** The use of Secure Communication in sharing of sensitive information is strictly confidential. Any unauthorized sharing of such information may be considered a breach of confidentiality.

- **Clear to Zero:** All employees and Independent Contractors are required to clear the FirstPage or Dashboard of all numbers in their Therap accounts at the beginning of their shifts. Employees' and Independent Contractors' FirstPage or Dashboards can be cleared by opening and reading all information contained in these links. Employees and Independent Contractors are responsible for all information contained in these communications. The Therap system does record that these items have been viewed and acknowledged by employees and/or Independent Contractors. *Initial*____________

- **Printable Format or Record Access:** Information contained in Therap is printable and can be reproduced, upon request, for any quality monitor, licensing employees, survey teams, auditors, or guardians.

- **Readily Accessible:** Therap will be accessible, upon request, to any authorized person including licensing employees, investigators, surveyors, auditors, and monitors, twenty-four hours per day. Metro Support Services, Inc. Administrators can provide immediate and complete access to the clients' electronic records to authorized personnel through online access and remote approval. The list of Metro Support Services, Inc.Administrators is available under each user's "My Account" section located on their FirstPage or Dashboard.

- **Deletion of Information:** Therap will maintain all data submitted by users, in the original form, and as approved, updated or modified, all versions of reports, data, and information will be archived and retrievable. Any sensitive or confidential documents, e.g., Abuse, Neglect, Unlawful Acts, etc., will be available upon request by authorized personnel to review, and may be accessed online with restricted access. Records and data will not be deleted from the system, and any such requests for the deletion of any information will be recorded and accessible to auditors, investigators and appropriate authorities. This information will be recorded in Administrators' Secure Communications, and will contain a written explanation of the request, with identification of users making the requests, dates and times, data information, and Form ID numbers.

____________________________________ ____________________

Staff Signature Date

____________________________________ ____________________

Staff Signature Date