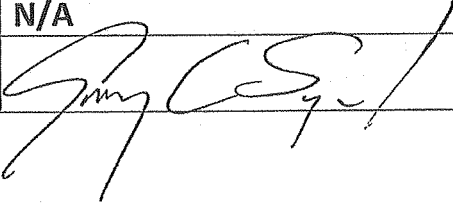


Standard Category	Administrative
Standard Title	Electronic Data Management
Regulations	CMS Electronic Signature Guidance Health Insurance Portability & Accountability Act of 1996 (HIPAA) Uniform Electronic Transactions Act (UETA) E-SIGN (The Electronic Signatures in Global and National Commerce Act) OPWDD Policy Statement on Electronic Signatures and Records
Original Issue Date	March 7, 2011
Latest Revision Date	
Number of Pages	10
Attachments	N/A
Approved by: Gary Siegel, Executive Director	

POLICY

Catholic Charities Disabilities Services shall use an electronic data management system for documentation and file management.

PURPOSE

To comply with state of New York Medicaid & Medicare Documentation standards, DHS Policy, 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 for the agency. The agency'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 staff. 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, periodic reports, etc.

DEFINITIONS

- Direct Care Professional (DSP) – those persons employed who provide direct care for consumers
- Individual Support Plan (ISP) – Plan used to provide information on individuals served.
- General Event Report (GER) – Used to report unusual events, accidents, or situations taking place outside of the norm.
- Behavior Plan (BP) – Information used to assist with behaviors used by those individuals served
- Individual Data Form (IDF) – form containing pertinent information regarding the individual served.
- Emergency Data Form (EDF) – form listing medical information of the consumer to include current medications etc, to be printed and transported to medical facilities.
- T-Logs – case notes and contacts documenting supports provided to consumer.
- ‘Generated by’ – the individual staff member creating a PDF, Excel file or creating a summary report within Therap to be printed or saved.
- ‘Created by’ – the person providing the direct support service and responsible for the creation of the service documentation.
- User – An agency employee who has an account in Therap created for their use.
- Provider Administrator – Agency employee who administers the agency’s use of Therap through a Provider Administrator User Account administered by Therap.

PROCEDURE

Agency staff will be trained in the following procedures:

1. Protected Health Information (PHI) of individuals should always be communicated securely, for example using secure HTTPS, a cryptographically secured protocol and interfaces.
2. Staff will be instructed in the authorized use of PHI for the individuals in their care and not to discuss confidential information outside of their place of employment.
3. Users need to proceed with caution when they are saving electronic files containing PHI or files exported from Therap to Excel or PDF in a shared computer.
4. Users should not share their personal login information with others.
5. Therap passwords will contain eight (8) characters to include at minimum one upper case letter, one lower case letter, one numeral, and one symbol.

6. Users should not write down their login information on paper or save them in an electronic file that can be accessed by other users.
7. Users Therap password should be different from the password they use to log into a computer.
8. Provider Administrators will establish a password policy for the agency.
9. While accessing the system from a shared computer or a public place, user should not leave the computer screen unattended, and delete all information from those computers, including clearing caches cookies and temporary files.
10. All agency employees are advised to not store data on agency or personal computers, laptops or other storage devices; the files containing PHI should be deleted after the work has been completed.
11. Management Reports, Behavior Information, Nursing, Summary Reports and other reports containing PHI may be printed or copied for use as required for agency business, as provided in state or federal regulation and agency policy.

Provider administrators will be trained by Therap Services staff in the use and management of electronic data within the secure database. These selected Provider Administrators are the persons responsible for proper assignment of access privileges to users, setting up password policies and activating/deactivating user accounts. They will be required to have a clear understanding and sound knowledge about the various application capabilities and the underlying HIPAA regulations and E-sign policy. These include:

Access Control: Administrators are responsible for assigning proper roles and privileges to users to grant them access to the system while at the same time restricting that access only to the information they are authorized to see. Provider Administrators are also responsible for updating these access privileges assigned to users in accordance with their changing job responsibility and authority. An administrator will be notified immediately when someone is terminated and their use privileges will be deleted from the Therap system.

Implement Password Policy: Provider Administrators are able to set up and implement a suitable password policy for the agency by specifying a number of properties including the minimum length, number of letters, digits, and special characters required and the policy regarding the expiration period of passwords. The Agency shall not record, inquire of any employee or assign passwords to employees. The agency may reset a temporary password at the request individual employee who has been locked out of the system. The employee will be prompted and requested to reset their temporary password by the Therap System.

Managing User Accounts: Provider Administrators are responsible for creating and activating Therap accounts for employees and providing them with the login information they need to access these accounts. Provider Administrators need to instruct new account holders to choose a new password for themselves once they start using the system. If a user forgets his password, login name or provider code, they will have to go to their respective Provider Administrators to collect this information (Therap Customer Support will not alter or supply users' login information, except for agency Provider Administrators.) Providers Administrators may also disable an employee's user account when they are leaving the organization, on extended leave, or administrative leave.

Assignment of Roles and Caseloads: Therap implements a multilevel access mechanism based on roles and individuals. Providers can specify the level of access available to a particular user of the system and grant permission accordingly. This only allows users to have access to information they are authorized to work with. Provider Administrators shall assign each User a specific list of roles for access privileges as well as access to a specific caseload(s) of individuals based upon their need to know, access and level of responsibility for those individuals.

Access to Therap during Non-Work hours: All Non-Exempt and Direct Care Employees shall be instructed not to access Therap during non-scheduled work hours. Employees are not required by the agency and are not authorized to access the Web-Based Electronic Data Management System during non-scheduled work hours.

Message Integrity: All communications between end users browser and the Therap application is carried over HTTPS, a cryptographically secured protocol. No third party can modify the data transferred. No user can 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 the user to the Therap system use SSL, and thus are secure during transmission

Non Repudiation: As the data is stored securely no user can access the data without proper privilege and audit trail (activity tracking), no user can deny the association of his/her identity with a document stored in Therap.

User Authentication: All users, including Therap staff, 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, before starting to enter information again. The system displays a countdown message for 5 minutes before the session actually expires; if the user wants 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 people from using your login in cases where users may have left the program without logging out.

Alerting over Non-Secure Media. One challenge to security is the use of non-secure media, such as email, text messaging, and paging. The Therap system assures that no Protected Health Information is transmitted over these media, 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 Protected Health Information. When secure media, such as SComm and FirstPage, are used for alerting, the system allows Protected Health Information, such as the individual's name, to be included.

Tracking User Activities: Provider Administrators are able to track all 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 within an agency. The Activity Tracker shall record all Users accessing the system, time, date, login name, User Name, IP address used to access the system, all activity, including viewing of information, creation or modification of any and all data or records. Provider Administrators with this role or option can detect any attempts to breach the system security (failed login attempts) and other misuse. The Therap system is monitored by security systems and staff for unusual activity within the accounts. Therap Services will provide training and support materials for Provider Administrators to learn about these and other HIPAA compliant Therap features, as needed.

Staff Training: The agency will provide training of all new employees in the use of Therap, methods and requirements for documentation and the use of searches, summary data and reports for all modules. Online training, "walkabouts", automated training, webinars, a User Guide, online help, Feedback, FAQs, etc., are available for all users on: www.TherapServices.net

Clear to Zero: All employees are required to clear the FirstPage or Dashboard, of their Therap account each day at the beginning of their shift of all numbers, which are notifications of new information about the individuals in their care or important communications from the agency, DDS or others. The employee's FirstPage or Dashboard can be cleared by opening and reading all information contained in these links. The employee is responsible for all information contained in these communications and the Therap system does record that these items that have been viewed and acknowledged by the employee.

Printable Format or Record Access: All information contained with The Electronic Data Management System (Therap) is printable and can be reproduced upon request for any Quality Monitor, Licensing Staff, Survey Team, Auditor or Guardian upon request.

Readily Accessible: The Electronic Data Management System (Therap) shall be accessible to any authorized person including licensing staff, investigators, surveyors, auditors and monitors upon request, twenty-four hours per day. The Provider Administrator of the agency can provide immediate and complete access to the electronic records of all individuals to an authorized person, through online access and remote approval. The list of Provider Administrators for the agency is available to all employees under their "My Account" section located on their FirstPage or Dashboard.

Deletion of Information: The Electronic Data Management System (Therap) shall maintain all data submitted by the Users, in the original form, and as approved, updated or modified, all versions of reports, data and information shall be archived and retrievable. Any sensitive or confidential documents (Abuse, Neglect, Unlawful Acts, etc.) shall be available upon request by authorized persons to review and may be accessed online with restricted access. Records and data shall not be deleted from the system; any such requests for the deletion of any information shall be recorded and accessible to auditors, investigators and appropriate authorities. This information shall be recorded in the Provider Administrators' Secure Communications, and shall contain a written explanation of the request, with identification of the User making the request, Date and Time, data information, and Form ID number.

Electronic Communications Systems: Computer facilities owned, leased or otherwise maintained by the Company are intended for use by qualified and authorized personnel and only in the conduct of official business.

It is important that every employee understand that all electronic communication systems used while at work, including but not limited to the Internet, telephone systems and e-mail, as well as all information transmitted, received or stored in these systems are the property of Catholic Charities Disabilities Services. Thus, Catholic Charities Disabilities Services needs to be able to access and/or disclose any information in the electronic communication system, even those protected by your personal password, at any time, with or without notice to the employee. Employees have no expectation of privacy in connection with the use of these systems or the transmission, receipt or storage of information in such systems. Therefore, employees should not use these electronic communication systems to store or transmit any information that they do not want management and/or other employees to see, hear or read.

Employee's communication through these electronic communication systems must always be handled in a professional and ethical manner since it reflects on Catholic Charities Disabilities Services, our customers, prospects, competitors, suppliers and other employers. Nothing should be communicated through the electronic communication system that would be inappropriate in any other medium or form of business communication. Specifically, the electronic communications systems are not to be used in a way that may be disruptive, illegal, offensive to others or harmful to morale. Each employee is responsible for abiding by copyright and trade secret laws in the use and transmission of information.

The use of derogatory, inappropriate, discriminatory and/or non-professional communication, including but not limited to slander, harassment of any type (sexual, racial, etc.) or obscenity is prohibited. Similarly, there is to be no display or transmission of sexually explicit images, messages or cartoons.

All data contained in this system is Catholic Charities Disabilities Services property and should not be disclosed, accessed or manipulated for any purposes other than official business. No attempt should be made to override or deceive any security precautions assigned to the computer system. Employees are required to keep their passwords confidential, change them on a regular basis and to comply with all security procedures. The unauthorized use of a password, or the unauthorized access to or retrieval of information transmitted or stored in the electronic communication system is strictly prohibited.

ELECTRONIC SIGNATURE CRITERIA

- A. Identify the individual signing the document by name and title.

Once a user logs into the Therap system, the name and title for that staff member is recorded on every form s/he saves or submits into the system.

- B. Date and time electronic "signature" is affixed.

The date and time stamp is also affixed on each form that is saved, submitted, updated or reviewed by the user.

- C. Assure the documentation cannot be altered after the signature has been affixed by limiting access to the documentation.

Once a form has been saved in Therap, no user can make changes to it without proper access privileges. Also, any changes made to the documentation can be tracked as the previous forms of the documentation are archived in the system.

- D. Provide substantial evidence that makes it difficult for the signer to claim the electronic representation is not valid.

Provider Administrators produce the Activity Tracking report to show which actions were performed by the staff members at what times and from which computers.

- E. Ensure exclusive access and use of the computer password.

Provider Administrators are responsible for creating and activating Therap accounts for employees and providing them with the login information they need to access these accounts. Provider Administrators instruct new account holders to choose a new passwords for themselves once they start using the system. If a user forgets his

password, login name or provider code, they will have to go to their respective Provider Administrators to collect these information (Therap Customer Support does not know users' login information, except for provider administrators.) Providers Administrators will deactivate an employee's Therap "User" account, upon the person being suspended, place on administrative leave or terminated from employment.

ELECTRONIC DOCUMENTATION

- A. Meet all documentation and signature requirements contained in the Medicaid Provider Manual

The Agency has read and does understand the requirements stated in the Medicaid Provider Manual and the agency will comply with those policies.

- B. Meet all documentation and signature requirements specific to the program and services provided.

The Agency is aware of the documentation and the signature requirements of the Medicaid Assistance Program and complies with them.

- C. Assure the documentation cannot be altered once entered.

Once a user logs into the Therap system, the name, title, date and time stamp for that staff member is recorded on every form s/he saves or submits into the system. Without proper access privileges, no user can make any changes to the documentation.

- D. Maintain a system to document when records are created, modified or deleted to provide an audit trail.

The Activity Tracking application of the Therap system keeps records of operations performed by people using the Therap system. This security option lets you find out who has been using the system, when they were using it, where they accessed it from and what was done. This tool is used by the Administrator/QA to ensure documentation is done in a timely manner and occurs where it should.

DOCUMENTATION AND MONITORING OF DATA ENTRY

- A. Documentation of the services and care provided and attendance reports shall be made web based on the Therap Services electronic data management system utilized by the Agency. This web based system is maintained by Therap Services and monitored internally, utilizing the Activity Tracking system, Summary Reports and search features by Administration, Health Services and Quality Assurance. The Agency will establish a pass code access policy, assign employee roles, create CaseLoads for assignment to employees and ensure timely entry of case notes and care provided as required by the provider manual.
1. Users need to be identified and authenticated before they are logged into the Therap system. Users have to use a unique combination of their Login Name, Password, and Provider Code to log into the Therap system.
 2. The Therap Provider Administrator will be able to configure a password management policy for user accounts. They also have the option to track user activities taking place within the organization using the Therap system. They can find out who have been using the system, when and for what purposes.
 3. In Therap, all the data entered are time and date stamped. In cases where updates are made to the data that has been entered, the original data is archived in the system and is easily accessible by the Administrative staff. Every follow-ups, reviews or updates made to any form are also time and date stamped.
 4. Users of the Therap System are assigned with a standardized job classification or position and are assigned with what we call a Super Role, to be able to access the Therap System. Each option of the Therap applications has an associated Role. A Super Role combining one or more of these Roles can be created by the providers to enable their staff to adequately perform their tasks using the Therap system.
 5. Employee's access is set up and monitored by the Quality Assurance staff and the Program Administrator. The Administrator shall assigned administrative access to the Therap system. All information entered is date and time stamped to include reports, reviews, updates, and follow up.

6. Case/Service Notes (T-Logs), and ISP Data entries will be reviewed by Administration/QA staff to ensure accuracy of required documentation, timeliness of data entry and that PCSP needs and goals are being met. The QA will alert the supervisor of any documentation failing to meet standards and the agency will provide additional training and or appropriate personnel actions.
7. The QA reviews all GER's (Incident Reports) and takes the appropriate action to insure the required parties are notified of the event and those agencies requiring the information and assure that follow-up is completed and plans of corrective action are implemented.