Policy Number:
3
Effective: May 1, 2008
Revised: April 20, 2009, April 19,2010,
October 16, 2017, April 9, 2020

Subject: Client Records

PURPOSE:

Camden County Developmental Disability Resources (CCDDR) shall have a policy to have an official record for each client served by the agency.

POLICY:

The client record is the property of CCDDR and is maintained for the benefit of clients,their responsible parties, and CCDDR staff. CCDDR will maintain the security and confidentiality of client records and safeguard the information contained in the client record against loss, tampering, or use by unauthorized persons. The content and format of client records are standardized according to joint Division of Developmental Disabilities (DDD) and Senate Bill 40 Targeted Case Management guidelines to facilitate:

- Accessing client information
- Maintaining/Filing records
- Charting accurately and punctually
- Auditing/Reviewing records
- Consistency among staff making entries into records

Official Records

An official record for each client served by CCDDR shall be maintained within the CCDDR facility and in the CCDDR secured online network (aka "cloud") database. The content and format of the client's official record will contain separate sections including, but not limited to, the following categories of information:

- Client admission/discharge/transfer information
- Legal documents
- Individual Support Plan (current and historical)
- Monthly/Quarterly reports
- Correspondence
- Financial information
- Assessments/Evaluations
- Health information
- Other pertinent information

Support Coordination log notes are recorded and stored in a separate online database used for Targeted Case Management service activity and billing.

Location of the Client Records

CCDDR shall follow the DDD Standardized Record as outlined in Appendix A. Any permanent physical (i.e. "paper") records of all clients served by CCDDR will be located in a secured area within the CCDDR office. The physical records shall be stored in an area reasonably protected against breaches in confidentiality, water damage, and other hazards. Digital records shall be stored on CCDDR's secured online network database, and Targeted Case Management activity shall be stored in the separate online database with all appropriate access and security protocols in place.

Support Coordinators can maintain temporary working files for physical records to be stored in a locked file cabinet for all clients on their caseload and a temporary working file for all clients on their caseload on the secured CCDDR online network database for digital records. At the very least, the working file(s) will contain pertinent documents within the current plan year or as necessary for immediate reference.

Applicable historical physical records shall be stored in the CCDDR permanent client record in the client records room, and digital records shall be stored appropriately in the permanent client record on the secured CCDDR online network database or Targeted Case Management database. Support Coordinators shall provide the appropriate physical or digital documents to the Administrative Assistant and/or TCM Office Manager as needed for filing in the permanent client record(s).

Client physical records may be removed from CCDDR premises only in accordance with a court order, subpoena, statute, or transportation to another service site. When records are transported, the security and confidentiality of the record is the responsibility of the staff person who is transporting the record. Staff who remove records from CCDDR premises without authorization are subject to disciplinary action, including dismissal.

Retention and Destruction

CCDDR shall refer to the Department of Mental Health (DMH) Department Operating Regulation (DOR) 8.110, Retention and Destruction of Protected Health Information, for rules pertaining to storage, retention, and destruction of protected health information. There shall be no other CCDDR facility policies pertaining to this, and the DOR shall control.

CCDDR must maintain records in accordance with the standards set forth by their regulatory authorities, to include the following when applicable:

- CCDDR will retain all records pertaining to Targeted Case Management for 6 years after the close of the contract year unless audit questions have arisen with the 6-year limitation and have not been resolved (all records shall be retained until all audit questions have been resolved)
- HIPAA: requests for information – 6 years; records related to services – 6 years from date of service
- SB 40 Board records – 7 years
- DMH DOR 8.110: permanent retention for some; others for 6 years; records for minor children 3 years after they reach legal age (See Appendix B)
- Records not specifically identified as permanent or in a retention schedule will be kept for no less than 7 years

Transfer of Records

All paper records will be forwarded to the receiving Targeted Case Management agency/DDD Regional Office upon official acceptance by either:

- Hand delivery
- Mailed by USPS, certified with return receipt

Transfer of electronic records between CCDDR and DDD Regional Offices/Taregeted Case Management agencies will be done via a folder system (FTP site) for the secure transfer of multiple types of reports and data. CCDDR is assigned access credentials and will transfer the information through a folder structure on DMH's secure FTP server. Records may be transferred directly to the agency which will be providing Targeted Case Management for the individual in the new location but must follow all transfer procedures listed in the Community Transition Manual to ensure the DDD Regional Offices involved are notified of the transfer.

Custodians of Client Information

The custodians of the client records at CCDDR shall be the Administrative Assistant and TCM Office Manager.

Access to Client Records

Anytime staff removes the physical client record from the client records room, the staff must check these out. The Administrative Assistant and TCM Office Manager shall maintain a check-out log form of all files checked out of the client records room. The Administrative Assistant and/or TCM Office Manager shall indicate on the check-out form, the time and date the file was checked out, what file was checked out, and to whom the file was checked out, which is also signed by the employee checking out the file.

All files checked out during the day by staff must be returned to the client records room at the end of the day to be re-filed. When the staff person has finished with the file, it is to be submitted to the Administrative Assistant or TCM Office Manager, who will log the time the file was returned and will refile the record. As a general rule, CCDDR Support Coordinators should only check out files for persons on their caseload.

Except in certain circumstances, clients served and/or their legal representatives have the right to review and obtain copies of medical/health information maintained in agency records and used for making decisions. Access to records, copying of records, changes to health information contained in the record, etc. shall comply with Policy 25, HIPAA Compliance, and Policy 26, Confidentiality of Client Informaton and Access to Client Records. Per Policy 25, HIPAA Compliance, the client or their legal representative must request in writing for access to inspect or receive copies of Protected Health Information, except in those instances covered by Federal Regulation and outlined in the Notice of Privacy Practices acknowledged at admission. It must further specify the exact information requested for access.

Copying

Paper copies of client record data can be made (if physical) or produced (if digital) by staff. These copies can be for their own client working file or to fax a document to ensure no original documents leave the facility. Staff removing paper documents from the file for copying/faxing are responsible for putting the file back into its original order and condition in which it was removed. Staff producing document copies from digital records are responsible for destroying the produced document copies after the intended purpose. Appropriate authorizations must be in place before CCDDR staff release confidential client information to outside entities.

Annual Audit of Records

The clients' permanent files maintained by CCDDR shall be audited annually by the Executive Director or appropriate designee(s) when the new annual plan is filed into the client record or as needed to ensure required documentation is in place per the state of Missouri and/or Federal Medicaid waiver guidelines. The audit shall determine if documents required per DDD and SB 40 standardized records management, as well as required Medicaid waiver documentation, are in place in all client files. A checklist or similar tool will be utilized to assist the Executive Director or appropriate designee(s) in the audit of client files. If there are missing documents in the client file, the Administrative Assistant, TCM Officer Manager, and/or assigned Support Coordinator shall make every effort to locate the missing data and/or documents.

During any annual audit of records, the Executive Director or appropriate designee(s) may determine if any original physical records/documents or physical copies of any original records/documents can or should be retained or destroyed according to the most recent applicable federal or state laws and pursuant to the most recent DMH Record Disposition Schedule.

REFERENCES:

- DDD Directive 1.060
- DMH DOR 8.110
- Targeted Case Management for Individuals with Developmental Disabilities Manual
- Developmental Disabilities Waivers Manual
- DDD Community Transitions Manual
- SB 40 Records Retention Schedule, MO Secretary of State's Office
- CARF Standards Manual

Appendix A

STANDARDIZED RECORD FILING ORDER

SKELETAL FILE **Originals at the Regional Office** **Copies to the TCM Entity**	**MASTER FILE** **Originals at the Regional Office** **Copies to the TCM Entity**
Admission Documents: • Initial Contact form • Application information • Application for Services • Initial Client Rights Receipt • HIPAA Form • Guardianship/Custody documentation • Assessments and Diagnosis supporting documentation used to determine eligibility (collateral) • Eligibility Determination, Intake Summary and Temporary Action Plans (if one is completed)	**Admission Documents:** • Initial Contact form • Application information • Application for Services • Client Rights Receipt • HIPAA Form • Guardianship/Custody documentation • Assessments and reports used to determine eligibility (collateral) • Eligibility Determination, Intake Summary and Temporary Action Plans (if one is completed) • Diagnosis supporting documentation
	Originals to the TCM Entity **No copies at Regional Office**
	PCP/IFSP/AMENDMENTS: • Amendments/Addendums to plan • Annual plan, to include budget summary plan • Behavior plan, if separate • Nursing Home Care Plan • Children's Services Case Plan (Children's Division Custody) • ICF-MR Form (requirement for Waiver Services) • Utilization Review Committee Recommendation sheet • Most recent progress reports (Judevine, therapies, etc.)
	Originals to the TCM Entity **No copies at Regional Office**
	REVIEWS: • 30 Day (monthly) program review completed by vendor for current IP year • Service Monitoring Review for current IP year • Current IP year of PCP reviews

Updated Documents to be sent to Regional Office Originals to Regional Office	Copies to the TCM Entity
EVALUATION AND ASSESSMENT: • Psychological Assessment • Any evaluation of documentation determining Diagnosis • Social History Assessment • Vineland/MOCABI/SIS • NHR – Nursing Home Reform Evaluation • Vocational Assessment • Diagnostic Summary (Special Education) • PT Evaluations • OT Evaluations • Speech Evaluation • School IEP	**EVALUATION AND ASSESSMENT:** • Psychological Assessment • Any evaluation of documentation determining diagnosis • Social History Assessment • Vineland/MOCABI/SIS • NHR – Nursing Home Reform Evaluation • Vocational Assessment • Diagnostic Summary (Special Education) • PT Evaluations • OT Evaluations • Speech Evaluation
	Originals to the TCM Entity **No Copies at Regional Office**
	HEALTH: • Physical Examination, including lab-work • Dental Examination • Audiological report • Consultation report and request (physician and hab center) • Physical reports and notes • Hospital discharge plan • Physician's orders and progress/program notes • Regional Center RN Health Inventory • Report of Hepatitis B Status • Immunization Records
	Originals to the TCM Entity – **No Copies at the Regional Office**
	CASENOTES: • Case Manager case notes/TCM log notes for 1 year (only until CIMOR access is gained)
Originals at the Regional Office	**Copies to the TCM Entity**
LEGAL: • Court Orders • Subpoenas • Guardianship Letters • Conservatorship Letters • Birth Certificate • Social Security Card • Missouri Medicaid/Medicare Card • Adoption Papers • Client Rights Receipt Form • Divorce Decree/Child Custody Documents • Consumer Marriage Certificate	**LEGAL:** • Court Orders • Subpoenas • Guardianship Letters • Conservatorship Letters • Birth Certificate • Social Security Card • Missouri Medicaid/Medicare Card • Adoption Papers • Divorce Decree/Child Custody Documents • Consumer Marriage Certificate

	Originals at the TCM Entity
	No Copies at the Regional Office
	LEGAL: CONTINUED • Annual Client Rights Receipt Form • Client Choice of Provider Statement • Notice of Right to Choose Form (Olmstead)
	Originals to the TCM Entity **No Copies at the Regional Office**
	FINANCIAL: • ISL Budget and Staffing Pattern • Individual Plan of Care (IPC Funding Authorization)

Appendix B

DMH DOR 8.110 (Effective 6-20-18)

PURPOSE: To ensure the availability of relevant data and information, it is the policy of the Department of Mental Health (DMH) to maintain specific retention schedules for various types of individually identifiable health information in compliance with federal and state laws and professional practice standards. DMH has a records disposition schedule approved by the State Records Commission. (RSMo 109.250) Under Missouri Statute 109.120, records may be photographed, microphotographed, photostated or transferred to other material using photographic, video or electronic processes, including a computer-generated electronic or digital retrieval system. This policy shall be consistently applied with the more stringent law followed and records destroyed after the retention period has expired.

APPLIES: DMH, its facilities and workforce.

PROCEDURE:

(1) Storage: All storage systems used by facilities within DMH shall be designed and implemented to ensure the safety, security, and integrity of consumer Protected Health Information (PHI). The storage method selected shall be dependent on the security of the area and the volume of the information stored.

(A) Paper PHI records storage shall be adequate to protect the physical integrity of the record and prevent loss, destruction, and unauthorized use.

1. If the records office is shared with other departments not responsible for maintaining the records, the shelves or file cabinets shall be lockable and kept locked whenever records staff is not in attendance.
2. If PHI records are retained in a lockable office that is not shared with other staff or in a separate locked file room, open shelf filing without lockable doors is acceptable. The office or file room shall always be locked when staff is not in attendance.
3. Storage area environment should not cause damage to the records and documents and shall meet accreditation and safety standards.
4. Off site storage shall meet the above standards, be approved by the facility or DMH Privacy Officer, as applicable, and have a signed business associate's agreement.
5. A record tracking system shall be in place to identify when a record has been removed, who took the record, and where it is located.
6. When a microfilmed copy of the original paper record has been produced, it may be used as a permanent record of the original. Duplicate reproductions of all microfilmed records shall be kept by the facility originating the paper records with suitable equipment for viewing and the original microfilm maintained off site in a fireproof vault. A log shall be maintained of all microfilmed records and cross-indexed, or otherwise linked with a common identifier, with the consumer Master Patient Index or Admission/Discharge database.

(B) Electronic: Electronic storage of medical records, if applicable, shall have a permanent retrievable capability, and such capability should occur even when there is a technology change.

(2) Retention: Retention of PHI records and databases shall comply with federal and state regulations; accreditation, licensure and accepted standards of practice. The more stringent between federal and state law shall be followed. This DOR shall be consistently applied and records destroyed after the retention period has expired.

(A) Master Patient Index: <u>permanent retention</u>

(B) Admission/Discharge Register or Database: permanent retention

(C) Medical Record: permanent retention as advised in the current Missouri DMH Records Disposition Schedule. Medical Record documents not on the schedule for permanent retention shall be kept six (6) years after the month of discharge or the month the Medicare cost report is filed, whichever is later, and for minors, three (3) years after the consumer reaches legal age as define by Missouri law.

(D) Consumer Financial Records: permanent retention per current Missouri DMH Records Disposition Schedule. These records include: consumer receipt and disbursement records, reimbursement information including but not limited to Standard Means Test, Consumer Financial File, placement files, resources files, valuable reports. Financial documents not on the schedule for permanent retention shall be kept six (6) years after the month the Medicare cost report is filed.

(E) Accounting of Disclosure of Information, a minimum of six (6) years according to the HIPAA Privacy Rule.

(3) Destruction: Destruction of PHI in paper or electronic format shall be carried out in accordance with federal and state law and pursuant to the DMH Records Disposition Schedule. Records approved for destruction must be destroyed so that there is no possibility of reconstruction of information.

(A) Paper: Microfilm is an accepted form of records maintenance and is recognized by Missouri Revised Statute Section 109.120 as an acceptable medium substituting original paper documents in legal proceedings. When paper records have been microfilmed the original paper may be destroyed. If they are not destroyed, then their retention shall be in accord with the procedures outlined in this DOR.

1. Because all media and reproductions typically have the same legal effect as originals, when a record meets the guideline for destruction, all copies in any medium shall be destroyed.

2. Appropriate methods for destroying paper records include burning, shredding, pulping, and pulverizing.

3. Documentation of the destruction of records shall include: Date of destruction; method of destruction; description of records; inclusive date of records; statement that the records were destroyed in the normal course of business; the signatures of the individual supervising and witnessing the destruction. Destruction documents should be permanently retained. Documentation records shall be maintained by the facility Privacy Officer, or the DMH Privacy Officer, as applicable.

4. If destruction services are contracted, the contract shall include a business associate agreement that specifies: the method of destruction; the time that will elapse between acquiring and destroying the records; identify safeguards against breaches in confidentiality; indemnify the facility from loss due to unauthorized disclosure; and provide proof of destruction to the facility Privacy Officer or DMH Privacy Officer.

(B) Electronic. When electronic records or computerized data is destroyed, it shall be permanently and irreversibly non-retrievable. For procedures for the destruction of computer disks, laser disks, back-up tapes, etc., please refer to the destruction requirements as set forth in DOR 8.370.

(4) Any questions as to whether information retention or destruction is permitted or required by law shall be directed to the Facility Health Information Management Director (HIMD), the Client Information Center representative, or the facility Privacy Officer or his/her designee. Electronic data destruction questions shall be directed to the Chief Security Officer or designee.

(5) There shall be no facility policies pertaining to this topic. The Department Operating Regulation shall control.

(6) SANCTIONS: Failure to comply or assure compliance with the DOR may result in

disciplinary action, up to and including dismissal.

(7) REVIEW PROCESS: Information shall be collected from the facility Privacy Officers annually to monitor compliance and identify any issues with this DOR

HISTORY: Emergency DOR effective January 15, 2003. Final DOR effective June 1, 2003. Amendment effective July 1, 2006. On July 1, 2009, the sunset date was extended to July 1, 2012. Amendment effective June 27, 2012. Amendment effective June 17, 2015. On June 20, 2018, the sunset date was extended to July 1, 2021.