



Division Directive Number

1.060

Effective Date: 12.04.09

Reviewed: 12.15.10; 08.20.13

Revised: 01.01.13

*Bernard Simons*

Bernard Simons, Director

**Title:** Procedures for Review, Retention and Management of Individual Records

**Application:** Applies to Regional Offices, Senate Bill 40 Boards, and other not-for-profit Targeted Case Management Entities

**Purpose:** To ensure the proper and consistent management, handling, and retention of individual records in compliance with federal and state laws and professional practice standards; to ensure accessibility and confidentiality of records in compliance with HIPAA regulations.

## SECTION I. RECORDS MANAGEMENT: STORAGE, RETENTION & DESTRUCTION

Please refer to HIPAA 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 facility policies pertaining to this topic. The Department Operating Regulation shall control.

Targeted Case Management (TCM) providers may retain either paper records or electronic records. When electronic records are utilized, electronic signatures will be accepted where a signature is required. Paper records may be destroyed if they have been converted to electronic records in such a fashion as to create an exact duplicate, (i.e. records have been scanned). All TCM providers utilizing electronic record keeping systems must have a disaster recovery plan in place in accordance with HIPAA regulation 45 CFR 164.308 (a) (7).

It is suggested that TCM providers developing electronic record keeping systems adopt the same standard filing order to maintain consistency statewide and to facilitate transfers between Regional Offices and TCM entities in different locations. The recommended electronic filing order is listed in Appendix A.

It is recommended that the TCM provider retain the following:

- Current individual file, with documents for 1 year
- Historical file to be returned to the Regional Office after 7 years, either in paper format or via electronic transmission

Various sources require different retention schedules. CARF and CQL require agencies to follow the policies of the funding source:

- TCM Manual – Medicaid may audit 5 years back
- Waiver Manual – Providers must retain records for six years from the date of service
- HIPAA – Requests for information – 6 years; Records related to services – 6 years from date of service
- Medicare – Providers' records -5 years
- SOS for SB40 Boards – 7 years

- DOR8.110 – Permanent Retention for some; others 6 years; records for minor children 3 years after they reach legal age
- Division of Medical Services – 5 years from date of service

When transferring records to a TCM agency, the Regional Office shall retain the original copy of the following documents in a working file: 1) All legal documents to include: Guardianship letters, Conservatorship letters, court orders, subpoenas, adoption papers, divorce decrees/child custody documents, marriage certificates, birth certificates, and 2) All admission documents to include: eligibility determination and admission information, assessments and reports used to determine eligibility, application information, client rights receipt, diagnosis sheet and supporting documentation, and most current NHRA screening.

If the Regional Office receives an audit or special request, the Regional Office will contact the TCM agency staff by email, advising specifics such as information requested, contact person to forward records to, and timeline for submitting the records. Records may be transmitted electronically to the Regional Office using the electronic records transfer process described below. If this process cannot be used by the agency sending the records, records can be sent via an encrypted flash drive or email.

## SECTION II. TRANSFER OF RECORDS

The procedure for administrative transfers between Regional Offices is described in Division Directive **5.010 Transfers & Portability of Funds Policy**. Once a transfer request has been accepted by Directive 5.010, the records shall be transferred to the receiving Regional Office and/or TCM agency.

All paper records will be forwarded to the Regional Office upon official acceptance of transfer by either:

- a. Hand delivery by TCM provider staff to Regional Office
- b. Mailed by USPS, certified with return receipt to Regional Office

Preparing paper records for submission to the Secretary of State’s office shall be the responsibility of the Regional Office.

Transfer of electronic records between Regional Offices and/or TCM providers will be done via a folder system for the secure transfer of multiple types of reports and data. All entities are assigned a four digit facility number by the ITSD Account Provisioning staff. This number is used to create a folder structure on DMH’s secure FTP server. Individual user accesses to these folders must be requested by using the DMH Access Request form and submitted via the Local Security Officer. An agency might not already have a facility number if they do not currently do any billing through CIMOR. An agency may request a facility number by filling out a DMH IT access form. Records may be transferred directly to the agency which will be providing TCM for the individual in the new location. For example, one TCM agency may transfer a record directly to another TCM agency, but must follow all transfer procedures listed in Division Directive 5.010 to ensure the Regional Offices involved are notified of the individual’s transfer.

All electronic records shall use the following naming standard when transferring the record:

LastName\_FirstName\_DMHID\_XXXX (where XXXX is the **RECEIVING** facility’s 4 digit number)

All documents to be transferred must be in PDF format and adhere to the naming standard. Additional identifying information such as file year may be placed after the set naming standard. An underscore must be used to separate the facility number and the additional information. For example, files named LastName\_FirstName\_DMHID\_XXXX\_2010 and LastName\_FirstName\_DMHID\_XXXX\_2011 could be used to transfer files for two different plan years. Or,

LastName\_FirstName\_DMHID\_XXXX\_Transfer\_Request could be used to electronically transfer the transfer summary and the accompanying documentation to the Regional Office.

### ***Process***

1. Documents to be transferred should be placed in the facility's **MRD/Send** folder on the secure FTP server. An example of the location would be: <https://ftp.dmh.missouri.gov/dmhftp/029/reports/mrd/send>
2. A program will run nightly to pick the files and or folders up and move them to their intended facility's folder. These will be titled <https://ftp.dmh.missouri.gov/dmhftp/1043/reports/mrd/recieved>
3. The sending facility will send an email to the receiving facility informing them that the document has been sent.
4. The receiving facility will see the files and or folders in their **Received** folder the next morning. The receiving facility, either Regional Office or TCM agency, will move the files and or folders to a folder specifically designated for storage of permanent original records, or convert the file to a paper file if the agency does not maintain an electronic record keeping system.
5. Files over 60 days old are deleted weekly. Files must be moved to another location within 60 days of receipt or they will be lost. It is the responsibility of the sending TCM agency to ensure that the process was completed and the transferred file was received by the receiving TCM agency.
6. The secured HTTPS website will only allow the upload of a single file at a time and will not accommodate the upload of an entire folder. However, there are two methods which may be used for sending folders. The sending agency may zip a folder into a file and send through the secure FTP server. Or the sending agency may purchase the FTP Voyager program which allows folders to be transferred.
7. Instructions for connecting to the secured ftp folders can be found on the DMH Public website, or click [here](#) for those instructions and additional information regarding purchase of the FTP Voyager program.

### ***Example***

Facility 029 needs a file and or folder to go to facility 1043.

1. Facility 029 names the file and or folder: SMITH\_JOHN\_12398743\_1043
2. Facility 029 places the file and or folder at the location <https://ftp.dmh.missouri.gov/dmhftp/029/reports/mrd/send>
3. The program will run overnight and pick up the file and or folder and place it at <https://ftp.dmh.missouri.gov/dmhftp/1043/reports/mrd/recieved>
4. The receiving agency will access the file and or folder, and move it to their permanent original records folder.

<b>SECTION III. PRIVACY AND SECURITY OF RECORDS</b>
---

All new Regional Office and TCM agency staff working near the location of PHI must receive HIPAA Privacy Training provided by their agency. All records must be maintained in a secured area. Examples: A room designated for records with a secure door, locked when no staff are present; or records placed in filing cabinets with a secure locking system. Records cannot be taken outside building, with the following exceptions:

- 1) Receipt of a court order which subpoenas the record
- 2) Record is being transported to the Regional Office upon discharge or transfer

3) An electronic backup being transported for storage at a second site

Each record is required to contain an access/checkout form where the date the file is accessed and the name of the staff viewing the record is documented.

**SECTION IV: CIMOR UPDATES**

Regional Offices will provide training to staff at TCM agencies utilizing CIMOR. TCM agency staff may request access to CIMOR roles in the DD Private TCM Provider Regional Office User group, allowing access to update demographic information in CIMOR. Staff at the TCM agency updating demographic information in CIMOR must also notify the Regional Office of the changes made.

Official documents such as birth certificates, court orders, etc., must be secured before making updates to CIMOR.

Regional Office and TCM agency staff may update an individual's diagnosis by forwarding a copy of the documents pertaining to the change in diagnosis, such as medical reports, evaluations, etc. to the Regional Office's diagnostician. The Regional Office's diagnostician will review the information and send documentation of the updated diagnosis to the Regional Office's Information Center staff for updating in CIMOR. The Regional Office will send the TCM agency a copy of the updated diagnosis summary.

The service coordinator will notify the Information Center of the death or discharge of an individual. In the case of an individual's death, the exact date of death shall be used as the official discharge date. All paper and electronic records maintained by the TCM agency will be returned to the Regional Office, with a Transfer Form.

**Authority**

- Division Directive 5.010 - Transfers & Portability of Funds Policy
- DOR 8.005 - Notice of Privacy Practices Procedures
- DOR 8.010 - Amendment of Protected Health Information
- DOR 8.020 - Consumer Right to Request Restrictions on the Use or Disclosure of Protected Health Information (PHI)
- DOR 8.030 - Access to Consumer Protected Health Information by Consumer, Parent, Guardian or Personal Representative
- DOR 8.040 - Access to Consumer Protected Health Information (PHI) by Department of Mental Health Staff, Volunteers or Students
- DOR 8.050 - Policy and Procedures for Obtaining Authorization for the Disclosure of Protected Health Information
- DOR 8.060 - The Provision of an Accounting of Disclosures of Protected Health Information to Consumers
- DOR 8.070 - Policy and Procedures for the Verification of Identity and Authority of Requestor
- DOR 8.080 - Ensuring Confidentiality of Protected Health Information for DMH Staff Working Away From a Facility Setting
- DOR 8.090 - Mandatory HIPAA Privacy and Security Training
- DOR 8.100 - Designated Record Sets
- DOR 8.110 - Retention and Destruction of Protected Health Information
- DOR 8.140 - HIPAA Complaint Process
- DOR 8.150 - HIPAA Minimum Necessary Standard
- DOR 8.160 - HIPAA Sanctions