MEDICAL TRANSPORTATION MANAGEMENT, INC.

Policy and Procedure

Dated:	July 19, 2004	**Policy No.** 437
Subject:	Transportation Provider Complaints, Grievance and Appeals Process	**Page** 1 of 3
Department:	Quality Management	

PURPOSE: To establish a transportation provider complaint, grievance, and appeal process that guarantees the right for a review of the determined outcome of a complaint or grievance to any of NEMT services.

POLICY: All complaints, grievances, and appeals received verbally or in writing are important and are channeled to the Quality Management Department for documentation, investigation, resolution, follow up, and reporting. Investigations of complaints, grievances and appeals are completed using applicable statutory, regulatory, contractual provisions and MTM's policies and procedures.

DEFINITIONS:
Complaint – A verbal or written expression by a transportation provider which indicates dissatisfaction or dispute with a recipient/member/beneficiary, MTM policy and procedure, claims, or any aspect of function.

Grievance – A written request for further review of a transportation provider's complaint that the party the complaint is against is unsatisfied with after completion of the complaint process.

Appeal - The formal mechanism which allows a transportation provider the right to submit any written expression of continued dissatisfaction after the written resolution of a grievance.

Transportation provider – MTM vendor providing the transportation service to a recipient/member/beneficiary.

COMPLAINT PROCESS:

1. A toll free number (866-436-0457) will be available for the recipient/member/beneficiary or their authorized representative to file a complaint.
2. A recipient/member/beneficiary or their authorized representative may file a complaint either verbally or in writing within one (1) year of the incident that resulted in the complaint or as otherwise determined by client contract.
3. All MTM personnel are trained to forward all calls and/or written correspondence regarding transportation provider complaints to the Quality Management Department where an assigned Quality Service Coordinator (QSC) will intake, document, investigate, resolve, follow up, and report the complaint.

Confidential

4. The QSC, if available, will answer the call at that time, document all information regarding the complaint, and if possible, resolve the complaint at the time of the call.
5. If the QSC is not available, the caller will be asked if they care to leave a message and receive a call back from the QSC.
6. If the caller does leave a message, the QSC will return the call the following business day.
7. The QSC will then begin the investigation, resolution and follow-up process. A thorough investigation will be conducted of each complaint using applicable statutory, regulatory, and contractual provisions, as well as MTM's written policies.
8. QSCs work with transportation providers, clients, social workers, medical facilities, recipients/members/beneficiaries and MTM personnel to resolve complaint.
9. MTM shall ensure that those making decisions on complaints are individuals who are not involved in any previous level of review or decision making that would prevent an objective, unbiased decision.
10. Complaints will be resolved within ten (10) days of their filing or otherwise identified by client contract.
11. The QSC will document and code all complaints in the NET Management System.
12. MTM shall maintain records of complaints, whether received verbally or in writing, that includes a short, dated summary of the problem, name of the complainant, date of the complaint, date of the decision, and the disposition.
13. The QSC will provide education to providers and recipients/members/beneficiaries as part of the resolution process.
14. The Quality Management (QM) Manager reviews the client's monthly complaint report prior to forwarding to the respective client.
15. QSCs use a standard format for reports sent to clients.
16. QM Department Staff maintains discretion and confidentiality in all complaint situations.
17. A transportation provider complaint summary will be forwarded to Network Management each month.
18. Complaints will be tracked and trended presented to the Quality Management Committee.
19. All MTM staff will immediately report all complaints of high visibility or potential serious consequence to the QM Manager who will involve MTM executive management as necessary.

GRIEVANCE PROCESS:

1. A *formal grievance procedure* is followed when a complaint resolution is not considered by the party the complaint is against to be satisfactory:
    a. The grievance must be sent to MTM in writing within ninety (90) days of the complaint resolution. Information must be specific and sufficiently detailed.
    b. MTM will acknowledge receipt of the grievance in writing via certified mail within ten (10) business days after receiving the grievance.
    c. A thorough investigation will be conducted of each grievance using applicable statutory, regulatory, and contractual provisions, as well as MTM's written policies.
    d. MTM will complete any necessary investigation and provide a written response to the complainant within thirty (30) days of their filing date. The notice will include the transportation provider's right to file an appeal.
    e. A corrective action may be part of the grievance resolution.
    f. All grievances will be reported to the client.
    g. All grievances are reported to the Quality Management Committee (QMC) on a monthly basis for tracking, trending, and quality improvement.
    h. MTM shall maintain records of grievances that include a copy of the original grievance, the response, and the resolution.

Confidential

APPEALS PROCESS:

1. A transportation provider may file an appeal.
2. The appeal must be in writing and must be filed within ninety (90) days following notification of a grievance decision.
3. The appeal may be filed by the transportation provider or the transportation provider's authorized representative.
4. All appeals are filed either with the Appeals Committee and/or State agency.
5. The Director of Compliance will perform the initial review of the appeal using applicable statutory, regulatory, and contractual provisions, as well as MTM's written policies.
6. The Appeals Committee composed of MTM's members of the Executive Management Committee and department directors or managers as appropriate will meet to make a decision.
7. Transportation providers or their authorized representatives will have the opportunity to present their case in person if requested to the Appeals Committee.
8. A corrective action plan may be included as part of the appeal's resolution.
9. A final decision will be reached within sixty (60) calendar days of receipt of the appeal with extensions possible if approved by the Appeals Committee.
10. A final written report will be issued and delivered by certified mail.
11. All appeals will be reported to the client.
12. MTM shall maintain all records of appeals and resolutions.
13. All appeals are reported to the Quality Management Committee on a monthly basis for tracking, trending, and quality improvement.
14. This policy is reviewed by the QMC on an annual basis for appropriateness and effectiveness.

APPROVED BY:

Director, Outreach and Compliance Date

President/CEO Date

Original Effective Date: 07/19/04
Revised: 3/7/05, 5/7/07
Next Scheduled Review: 07/19/05, 3/7/06, 5/7/08

Confidential

MEDICAL TRANSPORTATION MANAGEMENT, INC.

Policy and Procedure

Dated: October 2, 2008 **Policy No.** 413

Subject: Management of No Shows **Page** 1 of 3

Department: Quality Management

PURPOSE: To notify and educate members/recipients/beneficiaries who consistently fail to provide proper notification of cancellation of scheduled non-emergency transportation (NET) services.

POLICY: Weekly reports will be generated for members/recipients/beneficiaries with one or more consecutive no shows. An educational letter followed by a warning and education of suspension will be mailed to the member/recipient/beneficiary that accrued one or more no shows for the week.

DEFINITIONS:
X1- No Show- Member/Recipient/Beneficiary canceled direct to driver at pick-up.
X2- No Show-Member/Recipient/Beneficiary was not there at time of pick-up.
X3- No Show- Member/Recipient/Beneficiary was there but not ready.
S4- No Show- Return Trip Member/Recipient/Beneficiary was not arranged pick-up point.

PROCEDURE:
1. When a transportation provider reports that a member/recipient/beneficiary has not shown for a scheduled transportation service for one or more consecutive occurrences within a calendar month, the trip is coded in the NET Management System as a "member no show".
2. MTM's Business Solutions Group (BSG) will generate a batch of member/recipient/beneficiary no show letters on a weekly basis.
3. The report will contain the following information:
    a) The member/recipient/beneficiary name and Medicaid identification number; and
    b) The dates of the one or more consecutive no show occurrences
4. The Compliance Coordinator will review the member/recipient/beneficiary no show report, and review the following:
    a) The trip history for each member/recipient/beneficiary for whom a letter has been generated; and
    b) The trip note of each trip coded as a member no show (X1, X2, X3 and S4), within the designated month, to determine the accuracy of the member no show trip status.
    c) After the 2nd no show, the Compliance Coordinator will also attempt to contact the member/recipient/beneficiary and/or their caregiver or designated point of contact via telephone to receive further education on member no shows and trip cancellations.
    d) The Compliance Coordinator will maintain a monthly log of member no show reminder and warning notices.
        a. The Compliance Coordinator will compare each batch of member no shows letters within the designated month, to following monthly log of member no show reminders and warning notices, to determine if there are recurring patterns of no shows.

Confidential

e) The MTM Program Manager/Account Manager will receive notification of the member/recipient/beneficiary no shows.

5. The following steps will occur if the member/recipient/beneficiary receives one or more no shows:
   a) The first (1) valid member/recipient/beneficiary no show will result in an educational letter.
   b) If the member/recipient/beneficiary received a second (2) no show within 60 days, they will receive a warning letter.
   c) If the third (3) no show is received within 30 days from the second letter, the member/recipient/beneficiary will receive a letter of suspension from Medical Transportation for a period of 30 days.

This policy will be reviewed by the Quality Management Committee on an annual basis for appropriateness and effectiveness

APPROVED BY:

Manager, Quality Management and Compliance Date

Vice President, Operations Date

President/CEO Date

Original Effective Date: 10/5/2009
Reviewed/Revised: 2/11/10
Next Scheduled Review: 10/5/2010, 2/11/11

Confidential

Date
Member Name
Street Address
City, State Zip

Dear Beneficiary,

You requested medical transportation from Medical Transportation Management, Inc. (MTM) for the following date(s):

Trip Number	MM/DD/YYYY
Trip Number	MM/DD/YYYY
Trip Number	MM/DD/YYYY
Trip Number	MM/DD/YYYY

According to our records, a driver arrived to transport you on each date and you were not at the pick up location, canceled at the time of pick up, or were not ready when the driver arrived, which resulted in a "member no show." Please remember that you are responsible for canceling transportation services if you find that you do not need transportation on the requested date. To cancel transportation service, you may contact the transportation provider or MTM's Customer Service line used to request transportation, within 24 hours of the scheduled appointment date. Failure to do so may result in a lower level of service, for up to 30 days.

This is a formal notice that, if you fail to provide proper notice for the cancellation of any future trip that results in a "member no show," your transportation services may be changed to a lower level of service for up to 30 days.

If you are satisfied with this decision, a formal grievance procedure is available. You may contact the Quality Management Department at 1-866-436-0457 to inquire about our formal grievance procedure.

Sincerely,

Medical Transportation Management, Inc.

MTM, Inc.
16 Hawk Ridge Drive
Lake St. Louis, MO 63367

Confidential

MEDICAL TRANSPORTATION MANAGEMENT, INC.

Policy and Procedure

Dated: March 19, 2007 **Policy No.** 6450

Subject: Beneficiary Behavioral Issue Sanctions- **Page** 1of 2

Department: Quality Management

PURPOSE: To monitor beneficiary behavioral issues and establish a process to sanction beneficiaries which exceed the established threshold for beneficiary behavioral issues within a month.

POLICY: MTM will sanction beneficiaries that exceed the established threshold for reported behavioral issues within a month, through the temporary suspension of transportation services.

DEFINITION:
Minor behavioral issue: is an issue that creates discomfort or offends a driver or other Medical Assistance Transportation Program (MATP) passenger(s). An example can be screaming, disrespect, playing music, bringing animals other than service animals, littering the bus, use of foul language or actions etc.

Severe behavioral issue: is an issue that may create physical harm to the driver of other MATP passenger(s). An example can be striking another individual, creating disruption in the vehicle that could result in an accident, carrying a weapon, distracting the driver etc.

Verbal abuse issue: Verbal abuse is hostile language that hurts the listener and is not accidental. For effects of this policy, three verbal abuse issues will count as one *minor behavioral issue.*

PROCEDURE:
1. MTM representatives will document any reported issues of beneficiary abuse.
2. For minor behavioral issues:
    a. Quality Service Coordinators (QSC) will review and track reported issues of beneficiary abuse on a daily basis.
    b. When a minor behavioral issue is reported, the QSC will initiate an investigation that should be complete within the next 24 hours. If it is a substantiated complaint, the QSC will call the beneficiary or the beneficiary's guardian to notify that the beneficiary will be suspended from receiving transportation services. The suspension will vary depending in the number of minor behavioral issues reported within a month:

        - First issue reported: the beneficiary will be suspended for three calendar days
        - Second issue: the beneficiary will be suspended for seven calendar days
        - Third issue reported: the beneficiary will be suspended for thirty calendar days

CONFIDENTIAL

Additionally if a child leaves his/her designated seat to disturb other passengers or the driver, the child will be suspended from receiving transportation for the following day.

In all cases, a Suspension Notice letter will be mailed. The notice will outline the terms of the suspension.

3. For severe behavioral issues, depending on the nature of the issue, the beneficiary may be immediately and permanently suspended. A QSC will issue an Inappropriate Behavior Suspension Notice. The notice will outline the terms of the Permanent Suspension
4. The QM representative will place a note in the Red Flag of any beneficiary that has been issued a suspension notice, regarding the date span of the suspension, and the date the suspension expires.
5. This Policy is reviewed by the QMC on an annual basis for appropriateness and effectiveness.

APPROVED BY:

Manager, Quality Management	Date
Vice President, Operations	Date
President, CEO	Date

Original Effective Date: 03/19/07
Reviewed/Revised: 3/7/08
Next Scheduled Review: 3/19/08, 3/7/09

CONFIDENTIAL

MEDICAL TRANSPORTATION MANAGEMENT, INC.

Policy and Procedure

Dated: March 1, 2005 **Policy No.** 446

Subject: HIPAA Reasonable Safeguards
Incidental Uses and Disclosures and Minimum Necessary Applications

Page 1 **of** 8

Department: Quality Management

OBJECTIVE: To maintain HIPAA compliance

POLICY: MTM shall incorporate reasonable safeguards, which shall support
Processes, which support reasonable safeguards regarding protected health information (PHI) and Confidentiality.

Definitions-
Protected Health Information-Means individually identifiable health information

Incidental use or disclosure- is disclosure that can not reasonably be prevented, is listed in nature, And that occurs as a result of another use of disclosure that is permitted under the HIPAA Privacy Rule.

Reasonable Safeguards- the maintenance of appropriate administrative, technical, and physical safeguards which protect against uses and disclosures not permitted by the HIPAA Privacy Rule (45 CFR 164.530 (c) which is identified as Attachment A of this policy.

Minimum Necessary- A key protection of the HIPAA Privacy Rule and is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function

PROCEDURE: MTM shall incorporate the following:

1. Avoid discussing recipient/member/beneficiary information when in public areas, such as hallways, dining areas, smoking areas and elevators
2. Protect recipient/member/beneficiary health information by assuring confidentiality- isolate or locking file cabinets
3. Staff may coordinate services within their work stations
4. Staff may discuss coordination of services over the phone as long as those services are within the realm of the business activities in which there is the appropriate access to information and both parties are communicating the information on a minimum necessary basis.
5. When leaving information regarding protected health information or other confidential information on voicemail, leave only MTM's name, staff's name, phone number and ask that the individual call back

Confidential

6. All accidental disclosures of health information shall be reported to the Quality Management Manager (or designee).
7. Accidental protected health information disclosures shall be logged and reported monthly to MTM's legal counsel and as identified within specific client contracts. Please see Attachment B - Accidental Disclosure Reporting Form.

   Note: Addendums are attached to identify differences in specific client contracts

APPROVED BY:

Manager, Quality Management	Date
Vice President, Operations	Date
President/CEO	Date

Original Effective Date: 3/21/05
Reviewed/Revised: 4/10/06, 5/7/07, 3/7/08, 2/16/09
Next Scheduled Review: 3/21/06, 4/10/07, 5/7/08, 7/31/07, 3/7/09, 2/16/10

Confidential

Attachment A

Reasonable Safeguards

164.502 Uses and disclosures of protected health information: general rules.

(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) Pursuant to and in compliance with a consent that complies with § 164.506, to carry out treatment, payment, or health care operations;

(iii) Without consent, if consent is not required under § 164.506(a) and has not been sought under § 164.506(a)(4), to carry out treatment, payment, or health care operations, except with respect to psychotherapy notes;

(iv) Pursuant to and in compliance with an authorization that complies with § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), and (g).

(2) Required disclosures. A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and as required by §§ 164.524 or 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

(b) Standard: minimum necessary. (1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health

Confidential

information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) Minimum necessary does not apply. This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a) (1) (i) of this section, as required by paragraph (a) (2) (i) of this section, or pursuant to an authorization under § 164.508, except for authorizations requested by the covered entity under § 164.508(d), (e), or (f);

(iii) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(iv) Uses or disclosures that are required by law, as described by § 164.512(a); and

(v) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) Standard: uses and disclosures of protected health information subject to an agreed upon restriction. A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) Standard: uses and disclosures of de-identified protected health information.

(1) Uses and disclosures to create de-identified information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) Uses and disclosures of de-identified information. Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

Confidential

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) Standard: disclosures to business associates. (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).

(2) Implementation specification: documentation. A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) Standard: deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.

(g)(1) Standard: personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

Confidential

(2) Implementation specification: adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3) Implementation specification: unemancipated minors. If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(i) The minor consents to such health care service; law, regardless of whether the consent of another person has also been obtained; requires no other consent to such health care service and the minor has not requested that such person be treated as the personal representative;

(ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

(iii) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(4) Implementation specification: deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) Implementation specification: abuse, neglect, endangerment situations. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

Confidential

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) Standard: confidential communications. A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) Standard: uses and disclosures consistent with notice. A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) Standard: disclosures by whistleblowers and workforce member crime victims.

(1) Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a

Confidential

member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i

Confidential

ADDENDUM A: Children's Mercy Family Health Partners

1. Monthly reports of all PHI disclosure will be reported to FHP and FHK as per client request.

Confidential

MEDICAL TRANSPORTATION MANAGEMENT, INC.

Policy and Procedure

Dated: March 1, 2005 **Policy No.** 447

Subject: HIPAA - Physical Security Standards Private Health Information (PHI) and other Confidential Information **Page** 1 **of** 2

Department: Quality Management

OBJECTIVE: To develop and maintain physical security standards to help protect the confidentiality and privacy of MTM's recipient/member/beneficiary information.

POLICY: MTM shall follow a rigorous process to achieve and maintain secure work areas in which private health information as well as other confidential information is not compromised.

PROCEDURE:

1. Where feasible, workstations/terminals will be positioned or shielded so that computer screens are not visible to the general public or unauthorized staff.
2. Where practical, fax machines and copiers will be located in areas that are not accessible to the public.
3. Output from these devices should be monitored to insure that it is promptly delivered to the intended party or promptly discarded
4. Staff will secure their work areas when unattended. This includes breaks; lunch periods or any other times that work areas are vulnerable to snooping. If offices have doors that lock, they should be locked when unoccupied if Protected Health Information (PHI) is visible. Where no doors secure work areas, desks should be kept free of clutter, and all documents containing PHI should be placed in locked drawers or cabinets
5. Staff will enable a password protected screen saver feature to clear the screen if the workstation/terminal must be left briefly unattended.
6. Staff shall sign off/power off workstations/terminals when not in use or when leaving the work area, or at the end of the day.
7. Any electronic media being discarded or replaced (including hard drives in workstations) shall be written over, degaussed, or irrecoverably destroyed to ensure proper erasure of confidential or proprietary information
8. Staff shall secure media (such as hard copy, diskettes, etc.), which contain confidential information in double locked environment such as locked desk, cabinet, or room.
9. Management shall provide staff with facilities (shredders, secured bins, etc.) for proper disposal of confidential printouts. Staff shall dispose of printouts at these facilities.
10. Staff shall print documents only when necessary.
11. Copying of confidential documents shall be minimized.
12. Management and staff will take any other reasonable and logical measure necessary to maintain a secure work area, even if this measure is not specifically enumerated above

Confidential

APPROVED BY:

Manager, Quality Management	Date
Vice President, Operations	Date
President/CEO	Date

Original Effective Date: 3/21/05
Reviewed/Revised: 4/10/06, 5/7/07, 3/7/08, 2/16/09
Next Scheduled Review: 3/21/06, 4/10/07, 5/7/08, 3/7/09, 2/16/10

Confidential

MEDICAL TRANSPORTATION MANAGEMENT, INC.

Policy and Procedure

Dated: March 19, 2007 **Policy No.** 449

Subject: HIPAA – Electronic Security Standards **Page** 1 of 2

Department: Quality Management

OBJECTIVE: To develop and maintain HIPAA compliant security standards to ensure the confidentiality and privacy of recipient information upon electronic transfer.

POLICY: MTM shall follow HIPAA compliant processes to achieve and maintain secure transmission of data containing Protected Health Information (PHI).

PROCEDURE:

1. PHI will be communicated on as needed basis via employee emails which are housed within the MTM Server. In these circumstances minimal information will be contained within the email, i.e. if the recipient's/member's/beneficiary's name is attached, no other information which is identifiable will be attached such as recipient/member/beneficiary number or state identification number. Neither recipient/member/beneficiary name, recipient/member/beneficiary number or state identification number should be contained within the same email nor be communicated using email which is not submitted within a secured and protected environment (within MTM's server).
2. All outgoing emails for recipients outside of the MTM server must have HIPAA language attached to it.
3. When sending an electronic file containing PHI to recipients outside MTM's server, the sender must observe the following rules:
    a. If file size is larger than 10 megabytes, is must be placed in an FTP server.
    b. If the file is less than 10 megabytes, it can be sent either by secure email or by protected password Excel spreadsheet.
4. This policy is reviewed by the Quality Management Committee on an annual basis for appropriateness and effectiveness.

Confidential

APPROVED BY:

Manager, Quality Management Date

Vice President, Operations Date

President/CEO Date

Original Effective Date: 03/19/07
Reviewed/Revised: 3/7/08, 2/16/09
Next Scheduled Review: 03/19/08, 3/7/09, 2/16/10

Confidential

MEDICAL TRANSPORTATION MANAGEMENT, INC.

Policy and Procedure

Dated: May 7, 2007 **Policy No.** 452

Subject: HIPAA Training **Page** 1 **of** 1

Department: Quality Management

PURPOSE: To ensure all MTM staff are trained regarding the HIPAA regulations.

POLICY: All MTM staff will have initial HIPAA training within new employee orientation and ongoing HIPAA training on an annual basis.

Definition: HIPAA: Health Insurance Portability and Accountability Act

PROCEDURE:

1. HIPAA training will be part of MTM's new employee orientation agenda.
2. HIPAA training will include discussion of transactions and code sets (as applicable), and privacy and security.
3. Upon completion of HIPAA training, staff will sign HIPAA training and confidentiality statement Documentation of the training and copies of the confidentiality statement will be stored in Human Resources. Documentation includes sign in sheets, content of training and training dates.
4. Ongoing training will be provided as needed.
5. This policy is reviewed by the Quality Management Committee on an annual basis for appropriateness and effectiveness.

APPROVED BY:

Manager, Quality Management Date

Vice President, Operations Date

President/CEO Date

Original Effective Date: 5/7/07
Reviewed/Revised: 3/7/08, 2/16/09
Next Scheduled Review: 5/7/08, 3/7/09, 2/16/10

Confidential

MEDICAL TRANSPORTATION MANAGEMENT, INC.

Policy and Procedure

Dated: June 25, 2007 **Policy No.** 454

Subject: Electronic Communications – Compliance **Pages:** 1 of 12

Department: Quality Management

PURPOSE:

MTM's Electronic Communications Policy (the "Policy") outlines the processes and procedures that will be utilized by MTM to minimize risks and maximize benefits of Electronic Communications for MTM, its clients and their enrollees, members, insureds and/or covered persons (collectively, "Covered Persons"). This Policy should be reviewed in conjunction with MTM's Employee Manual.

The use of Electronic Communications Resources to transmit or maintain certain types of information, including, without limitation, Protected Health Information, is subject to federal law, state law, MTM's contractual obligations, and its existing policies, processes and procedures (including its Records Management Policies). The purposes of this Electronic Communications Compliance Policy are:

- to establish policies regarding the privacy, confidentiality and security of Electronic Communications which comply with MTM's obligations under federal law, including, without limitation, the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder ("HIPAA"), state law, MTM's contractual obligations, and MTM's existing policies, processes and procedures (including its Records Management Policies);

- to ensure that Electronic Communications and Electronic Communication Devices are used for purposes appropriate to MTM's business;

- to inform all MTM employees about the applicability of the laws regarding Electronic Communications;

- to ensure that Electronic Communications and Electronic Communication Devices are used in compliance with those laws and policies; and

- to provide guidance concerning MTM and its employees rights and responsibilities with respect to the proper use of Electronic Communications and Electronic Communication Devices.

POLICY:

MTM shall follow a comprehensive set of guidelines, processes and procedures, as described herein, to ensure the appropriate use of Electronic Communications and Electronic Communication Devices in compliance with federal law, state law, MTM's contractual obligations and its existing policies, processes and procedures (including its Record Management Policies). Any violation of this policy will result in an employee's discipline, up to and including termination.

SCOPE:

This Policy applies to any Electronic Communications that are transmitted or received by MTM and/or its employees, whether through Electronic Communication Resources owned or managed by MTM or otherwise.

AUTHORITY:

This Policy has been issued by MTM's Director of Compliance under the authority of MTM's Board of Directors and its Quality Management Committee. MTM's Board of Directors and its Quality Management Committee reserve the right to revise or withdraw this Policy and any rules, policies, or procedures under this Policy at any time in order to maintain efficient operations. MTM employees will be notified of any amendments to the Policy. MTM employees are expected to adhere to this Policy in a manner that is supported by MTM, and to exercise good judgment in the discharge of their responsibilities with respect to Electronic Communications and Electronic Communication Resources.

No part of this Policy is intended to supersede any legal or regulatory requirements. Changes to this Policy require approval by the Board of Directors of MTM. Changes in operational procedures, standards, guidelines and technologies, provided, they are consistent with this Policy, may be authorized by the Director of Compliance. The primary responsibility for enforcement of this Policy and its operational procedures rests with the Direct of Compliance and with Senior Management.

DEFINITIONS:

<u>Authorized Users</u>

Authorized User means any person who uses MTM's Electronic Communication Resources with proper authority. This term includes employees of MTM who have completed the required prerequisites for use such Electronic Communication Resources, as described below. This term does not include persons who are not employees of MTM or persons who are employees of MTM but who have either not completed the required prerequisites for use of such Electronic Communications Equipment or not been properly authorized to use such Electronic Communication Resources. Prerequisites for use of MTM's Electronic Communication Resources are as follows:

- An approved request for access signed by the employee's immediate

supervisor; and

- Completion of mandatory training in the use of MTM's Electronic Communication Resources by the employee

Each employee, including new hires, will receive training on MTM's Electronic Communication Resources by MTM's System Administrator with specific procedural training regarding security and controls (with an emphasis on employee responsibilities and rights in the use of Electronic Communication Resources). In some instances, temporary employees or outside contractor (collectively "Outside Users") may be given authorization to access MTM's Electronic Communication Resources. Outside Users will be given the same training and follow the same policies as MTM's employees with respect to their use of MTM's Electronic Communications Resources.

Electronic Communications

Electronic Communications are identified as the use of Electronic Communication Resources to transmit information about or relating to MTM, its clients or their Covered Persons, from MTM offices or MTM personnel or to receive information about or relating to MTM, its clients or Covered Persons, at MTM offices or by MTM personnel.

Electronic Communications Resources

Electronic Communication Resources are identified as the following:

- all electronic information processing and communications equipment employed by MTM or its employees for the purposes of doing MTM's business, including, without limitation, computers, fax machines, wireless email, Internet/Intranet/Extranet access accounts, storage media, network accounts, computer and email instant messaging accounts, and related equipment or documentations located at MTM's offices or disaster recovery site; and
- all electronic information processing and communications equipment employed by MTM or its employees for the purpose of doing MTM's business that is connected to or able to be connected to MTM's offices or disaster recovery site from locations outside of MTM's offices and/or disaster recovery site, including, without limitation, personal information processing and communications equipment and software.

Protected Health Information

Protected Health Information means information which:

- relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and
- identifies the individual or with respect to which there is a reasonable basis

to believe the information can be used to identify the individual.

INDIRECT VIOLATIONS:

MTM expects that MTM employees will be sensitive to the intent of this Policy and not attempt to do indirectly what this Policy prohibits directly, and will not employ means to defeat the goals this Policy is intended to achieve, even though those means may not be specifically mentioned within this Policy.

OWNERSHIP OF MTM ELECTRONIC COMMUNICATIONS RESOURCES AND INTELLECTUAL PROPERTY:

MTM owns or leases and has the right to specify the use of all of its Electronic Communication Resources. No MTM employee has property interests in any of MTM's Electronic Communication Resources.

All intellectual property developed or conceived by MTM employees during the term of their employment shall be considered "work for hire" and shall be the sole and exclusive property of MTM.

PERSONAL USE:

MTM's Electronic Communication Resources are a corporate asset and should be used primarily for legitimate business purposes. Personal use of MTM's Electronic Communication Resources is not forbidden, but such use:

- Must be limited and not affect work performance and normal business activity
- Must not directly or indirectly interfere with MTM's business operation
- Must not compromise the security or confidentiality of MTM's information and/or Electronic Communications Resources;
- Must not compromise the reputation of MTM; and
- Must not burden MTM with noticeable incremental costs.

Personal use of MTM's Electronic Communication Resources does not include uses which require substantial amounts of time, uses for the profit or economic gain of the employee personally or uses which would otherwise violate MTM's Policies regarding employee time commitment, all of which are strictly prohibited.

While limited personal use is allowed as described above, employees have no reasonable expectation of privacy when using MTM's Electronic Communication Resources for personal use because such use may be monitored and reviewed by MTM.

UNACCEPTABLE USE:

The following activities are unacceptable and are prohibited with respect to use of MTM's Electronic Communication Resources by Authorized Users. The list below is not exhaustive, but provides a framework for identifying activities which would

be considered unacceptable and prohibited for Authorized Users:

- Unlawful Activities – MTM's Electronic Communication Resources must not be used to engage in illegal or wrongful conduct.
- Personal Gain – MTM's Electronic Communication Resources must not be used for personal financial gain.
- Fraudulent Offers – MTM's Electronic Communication Resources must not be used to make fraudulent offers of services, products or items.
- Intellectual Property Infringement – MTM's Electronic Communication Resources must not be used in a manner that infringes on the copyright or other intellectual rights of any third parties.
- Unsubstantial Claims – MTM's Electronic Communication Resources must not be used to exchange gossip, rumors, unsubstantiated claims or personal information about others.
- Discrimination – MTM's Electronic Communication Resources must not be used to send discriminatory messages based on gender, race, age, sexual orientation, disabilities, religious beliefs, political beliefs or other basis that is protected under applicable law.
- Insensitive Language – MTM's Electronic Communication Resources must not be used to send messages containing offensive, derogatory or abusive language.
- Harassment – MTM's Electronic Communication Resources must not be used to conduct personal attacks on others or in a manner that may be construed as harassment or threats or defamation of character.
- Profanity – MTM's Electronic Communication Resources must not be used for profanity.
- Objectionable Material – MTM's Electronic Communication Resources must not be used to send or create pornography or sexually explicit jokes or material.

RESOURCE RESTRICTIONS:

Authorized Users shall not employ MTM's Electronic Communication Resources for purposes that could reasonably be expected to directly or indirectly cause excessive strain to MTM's Electronic Communication Resources, including, but not limited to, the following:

- Chain letters and malicious codes;
- Spam;
- Email bombs;
- Illegal software;
- DOS software;
- Automatic forwarding (do not set up rules to automatically forward email receive in an MTM email inbox to an external email box); and
- Source code (do not send computer source code via email).

EXTERNAL EMAIL SYSTEM AND PERSONAL ACCOUNTS:

- MTM related correspondence or any MTM related information must not be communicated or conducted via external email systems or personal email accounts.

- Accessing external email systems or personal email accounts through use of MTM's Electronic Communication Resources is prohibited.

CONFIDENTIALITY AND SECURITY:

Email Confidentiality and Security

Authorized Users should be aware that all Electronic Communications sent and received by MTM Authorized Users are protected by a "firewall", server and http address. Encryption software is also employed to further secure emails transmitted by MTM that contain Protected Health Information. Encryption will be used to the best of MTM's ability. In circumstances where encrypted information cannot be translated by the recipient; however, other avenues of Electronic Communications will be implemented or agreed upon.

In order to protect the security and confidentiality of email, Authorized Users must comply with the following guidelines:

- Authorized User should verify that they have selected the appropriate recipient or intended destination prior to transmitting an email message.
- Authorized User should not share personal mail boxes and passwords.
- Authorized Users should not leave email accessible when away from their desk so others can read or send a message from their computer, or amend or delete emails from their email account.
- Authorized Users will be responsible for all inappropriate email activity from their account.
- Authorized Users should retrieve printed email messages as soon as possible to prevent unauthorized individuals from reading messages containing privileged information.
- Authorized Users should not open emails from an unknown or unsolicited source. Such emails should be deleted.
- Authorized Users should not respond to any email that requests personal or corporate account information. Such emails should just be deleted.
- Authorized Users shall not communicate confidential, competitive or trade secret information of MTM to persons outside of MTM by Electronic Communications.
- Authorized Users shall not send email on which their name or electronic identification is hidden.
- Authorized Users are responsible for their own accounts and cannot provide their account number and/or password information to others.
- Authorized Users shall use email signatures to provide relevant contract information. Email signatures should contain the Authorized Users full name, job title, company name, telephone and fax numbers and MTM's web address.

- Instant Messaging is only to be used for MTM business with approval of the Manager, Technology Infrastructure & IP Telephony.
- Authorized Users must use email notices and fax notices when sending information to third parties that make clear any limitations on the extent to which the messages from the employee may have been understood to be sent on behalf of MTM.

Sample email disclaimer

This e-mail transmission is sent on behalf of MTM, and may be privileged, proprietary or confidential. It is intended only for the intended recipient. If you are the intended recipient or the person responsible for delivering this transmission to the intended recipient, please be advised that you are obligated under federal law, including, without limitation, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), to maintain the confidentiality of the information contained herein. In addition, please be advised that under federal law you may be prohibited from further disclosing this information unless you first obtain the written authorization of the person or persons named therein. In the event you disclose this information without first obtaining such authorization, you may be subject to various fines and penalties under federal law. If you are not the intended recipient or the person responsible for delivering this transmission to the intended recipient, you may not use, disclose, copy or distribute this transmission or take any action in reliance on it. If you received this transmission in error, please notify us immediately by telephone at (xxx-xxx-xxxx) or by email at yyy@MTM-inc.net, or by fax at (xxx-xxx-xxxx), and please dispose of and delete this transmission immediately. Thank you.

Sample fax disclaimer

This facsimile transmission is sent on behalf of MTM, and may be privileged, proprietary or confidential. It is intended only for the intended recipient. If you are the intended recipient or the person responsible for delivering this transmission to the intended recipient, please be advised that you are obligated under federal law, including, without limitation, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), to maintain the confidentiality of the information contained herein. In addition, please be advised that under federal law you may be prohibited from further disclosing this information unless you first obtain the written authorization of the person or persons named therein. In the event you disclose this information without first obtaining such authorization, you may be subject to various fines and penalties under federal law. If you are not the intended recipient or the person responsible for delivering this transmission to the intended recipient, you may not use, disclose, copy or distribute this transmission of take any action in reliance on it. If you received this transmission in error, please notify us immediately by telephone at (xxx-xxx-xxxx) or by email at yyy@MTM-inc.net, or by fax at (xxx-xxx-xxxx), and please dispose of, delete or return this transmission to us immediately. If you return this transmission by mail, we will reimburse your cost related to the transmission and returning it to us. Thank you.

Protection Against Malicious Code

MTM protects its Electronic Communication Resources with anti-virus software that scans for malicious code. Such anti-virus software is approved by the Manager, Technology Infrastructure & IP Telephony. All Authorized Users must reboot their computers and laptops daily in order for the anti-virus software to remain optimally effective.

- The System Administrator is responsible for seeing to it that the computers and laptops are running anti-virus software that included the current definitions of malicious code.
- If an Authorized User suspects that his/her computer or laptop has been infected by malicious code, he/she should not attempt to remove the malicious code without the assistance of the System Administrator or his/her designee. In the event an Authorized User suspects that his/her computer or laptop has been infected, he/she should immediately disconnect from all networks; call the System Administrator; and shut down the computer(s) involved.

Authorized Users are prohibited from disabling anti-virus software running on MTM-provided computers or laptops.

Password

Security passwords have been put into place to reduce potential unauthorized access to MTM's Electronic Communication Resources and Electronic Communications. The System Administrator will need to be contacted to unlock access.

- If an Authorized User suspects that his/her password has been disclosed to or learned by unauthorized parties, he or she must notify the System Administrator immediately and passwords must be immediately changed.
- Authorized Users should not store passwords in readable forms.
- Authorized Users should not send passwords electronically.

Email Encryption

MTM will make best efforts to encrypt Electronic Communications when required by contractual language or as is advisable under HIPAA. In circumstances where MTM has provided appropriate encryption and the recipient is unable to translate the encryption, MTM will suggest and/or provide alternative Electronic Communication formats, such as providing password protected Excel files, sending information that if compiled would be identified as PHI in separate emails so that PHI is not identifiable or in other mutually agreed upon formats. Authorized Users may encrypt their Electronic Communications with approved software provided by MTM. The software must provide MTM the ability for retention of any key necessary to access encrypted messages. Keys must be kept under the secure control of the System Administrator at all times.

Confidentiality

Confidential MTM information must be held in the strictest of confidence. Emails which contain confidential information should be identified as "CONFIDENTIAL"

within the subject line and/or apply appropriate password protection or encryption.

- Authorized Users should avoid using the confidential file names within the subject matter if the use of such names could disclose the confidential information.
- Authorized Users should not send files which are password protected in the same e-mail in which the password is sent. The password should be sent under separate e-mail and subject matter.
- Financial information and media inquiries are not to be disclosed or responded to by anyone other than the designated person and response should be provided within an approved medium.
- Employee information is not to be transmitted; all requests for employee information should be referred to MTM's Human Resources Department.

Portable Resources

Laptops, notebooks, palm pilots, PDA's, cell phones, cell phone/PDA combinations, and pagers are considered Electronic Communications Resources. Confidential information should not be kept on these devices. Further, these devices should not be used for long-term storage of MTM or customer data. Portable resources should be password protected and placed under lock and key when not in use. Portable resources will be configured with necessary controls and security features.

Remote Access and Uses

In certain circumstances MTM may permit certain Authorized User access to the MTM network to work remotely, either permanently or temporarily. In these circumstances, MTM may, in its discretion, provide MTM owned or leased Electronic Communications Resources to such employees for their use in working remotely ("Remote ECR"). All equipment, software and information stored within such Electronic Communications Resources are themselves considered Electronic Communications Resources and are the property of MTM.

- All Remote ECR must be returned to MTM prior to employee termination.
- Remote ECR must not be altered in any way without the System Administrator's approval.
- Any exchange of MTM data from the remote location network to MTM's network must be conducted using one or more security features or procedures approved by the System Administrator.
- Authorized Users must immediately report loss of or damage to Remote ECR.
- MTM reserves the right, with or without notice, to conduct inspections of the remote location from which any employee is working.
- MTM may withdraw an employee's privileges to work at a remote location if MTM is not satisfied with the security arrangements at the remote location.

MONITORING, AUDITING AND ACCESSING:

MTM has the right to monitor, audit, and access all files and messages transmitted from, received by or stored on MTM's Electronic Communications Resources in order to maintain and protect MTM's compliance standards, to ensure compliance with such standards, to ensure proper operation of the Electronic Communications Resources, to measure network activities and to identify suspicious activity. Monitoring is used to obtain information that is relevant to the workplace, but it may incidentally result in the monitoring of confidential personal information about an employee. Therefore, employees should have no expectation of privacy with regard to their use of MTM's Electronic Communications Resources.

Surveillance Software

MTM may use system software and system utilities to log, analyze and document the use of Electronic Communications Resources. Supervisors may receive reports generated from such software. The surveillance software may also be applied to transmissions with MTM's network from remote locations and portable devices. Systemic Electronic Communications Resources monitoring is allowed for business purposes, including employee supervision. All employees will be informed of such monitoring and will be asked to consent to such monitoring as a condition of employment.

Extent of Access and Disclosure

Authorized managers or supervisors may disclose private electronics communications or files of an employee to MTM for any valid business purpose. Employees will be informed of and required to consent to this Policy as a condition of employment.

MANAGING EMAIL:

All Electronic Communications exchanged between employees and internal and external sources are the property of MTM and must be stored in the original form and designated location.

Acceptable locations for storage are:

- Corporate Email server,
- PST files stored in the network corporate drives,
- Back-up tapes,
- Corporate Email archive,
- Employee's MTM – provided computer or laptop hard drive.

Accessible Data

All electronic data that is stored in the above stated locations are deemed accessible and discoverable in the event of legal discovery and regulatory investigations. Confidential and/or privileged data is protected and may be excluded from any requests.

Email Record Retention

MTM treats email as business records. Business records are subject to federal, state and local laws, as well as MTM's Records Management Policies. This Policy is not intended to replace MTM's current Records Management Policies, but to enforce an automated archiving system for emails as required by applicable regulations. Any email sent or received by MTM employees through use of MTM Electronic Communications Resources falls within this category. Email retention or archiving is a matter of regulatory compliance and is not to be used for ordinary operational purposes and is not a substitute for daily email management. MTM applies a consistent retention schedule to all electronic information; all electronic communications will be automatically archived for six (6) years with the exception of the following:

- Fiscal Correspondence – all information regarding revenue and expense shall be retained for seven (7) years.
- Legal Correspondence – such as business agreements, trademarks, and lawsuits are to be kept for seven (7) years.
- Sarbanes-Oxley Audit Records – all correspondence sent or received related to audit will be maintained for five (5) years from the end of the fiscal period of which the audit was conducted.
- Auditor Correspondence – all correspondence is to be retained for seven (7) years.

SUSPENSION OF RETENTION POLICY:

All electronic records which relate to an issue currently in litigation or which MTM has notice or should know of the potential for litigation will be retained as directed by legal counsel, regardless of the original retention schedule.

DATA DISPOSITION PROCEDURE:

MTM has implemented a process to periodically delete emails from the Authorized User's mailbox as follows:

- Deleted box – messages are automatically deleted after thirty (30) days.

- Outbox and sent box – messages deleted if older than thirty (30) days.

- In box – messages are deleted if they are older than ninety (90) days.

Disposition of Data from the Archive

Corporate data will routinely be disposed of after its retention period and upon the approval of the Systems Administrator and legal counsel. Electronic records relevant to anticipated litigation and those that are placed on litigation hold will be held until the litigation process is complete. If the litigation process is shorter than the record retention maturation timeline, the records will be held until the retention maturation date. If the litigation process is longer than the retention timeline, records will be held until the litigation process is completed.

REPORTING VIOLATIONS AND ENFORCEMENT:

Every Authorized User has the responsibility to report all suspected and known violations of this policy. All issues are to be immediately reported to the Manager, Technology Infrastructure & IP Telephony, so that prompt action can be taken. Any use of MTM Electronic Communications Resources by an unauthorized user is prohibited and should be reported immediately to the Manager, Technology Infrastructure & IP Telephony. Failure to confirm to this Policy or any provisions of it provides a basis for disciplinary action, up to and including termination of employment.

APPROVED BY:

Vice President, Operations Date

President/CEO Date

Original/Effective Date: 6/25/07
Reviewed/Revised: 3/7/08, 2/16/09
Next Scheduled Review: 6/25/08, 3/7/09, 2/16/10

MEDICAL TRANSPORTATION MANAGEMENT, INC.

Policy and Procedure

Dated: August 15, 2007 **Policy No.** 460

Subject: HIPAA – Recipient/Member Requests **Page** 1 of 2

Department: Quality Management

OBJECTIVE: To maintain HIPAA compliance, while allowing Recipients/Members to make special requests regarding their own Protected Health Information.

POLICY: Requests made by Recipients/Members related to their own Protected Health Information must be authorized by the Client as well as the Recipient/Member, adhering to State and Federal laws and regulations and in accordance with HIPAA 45CFR 164.530.

Definitions:
Protected Health Information (PHI) - individually identifiable health information.

PROCEDURE:
1. Requests for release of or amendments to a Recipients/Members PHI will be sent to the Quality Management Manager or designee.
2. The Quality Management Manager or designee is responsible for maintaining a log. The log will contain the name of the requesting party, the specifics of the request, the date of the request, the date the records were forwarded and by what means and any other notations regarding the request.
3. The Client must be informed of the request and written approval obtained prior to the release or amendment to a Recipients/Members PHI, considering that release or amendment of information may be contradictory to State laws.
4. When the Client has been informed and approval granted, the requested records (request not in response to risk or legal issues) are obtained under authorization of the Vice President of Operations or their designee.
5. When the Client has been informed and approval granted for an amendment to the Recipient/Member PHI, the Quality Management Manager or designee will see that the change is documented in the Recipients/Members file.
6. If the release of information is in response to a risk concern or other legal concern the request is discussed with the MTM President/CEO and General Counsel and all information received is forwarded to the President/CEO and General Counsel.
7. The request must be reviewed by the President/CEO and General Counsel to determine that all proper release forms have been supplied and the appropriateness of the request and response.
8. After review, the President/CEO and General Counsel will initial, date and return documents and comments to the Quality Management Manager or designee.
9. The Quality Management Manager or designee will forward the requested documents along with a cover letter to requesting party.

Confidential

10. In the case where an amendment to PHI has been made, the Quality Management Manager or designee will draft a brief letter to the requesting party, informing them that the changes requested have been made.
11. Recipients/Members can request an accounting of disclosures of their PHI, following the same steps and conditions as listed above.
12. The Quality Management Manager or designee will update the log.
13. This policy is reviewed by the Quality Management Committee on an annual basis for appropriateness and effectiveness.

APPROVED BY:

Manager, Quality Management	Date
Vice President, Operations	Date
President/CEO	Date

Original Effective Date: 9/28/07
Reviewed/Revised: 3/7/08
Next Scheduled Review: 9/28/08, 3/7/09

Confidential