Fraud, Waste, and Abuse (FWA) and HIPAA Training

UPDATED 2/6/2014
FRAUD, WASTE & ABUSE (FWA)
FWA Training Purpose

- Centers for Medicare & Medicaid Services (CMS) handed down new rules regarding FWA that must be followed by MTM, First Tier, Downstream & Related Entities
  - Providers, drivers & office staff
- Training required by CMS & MTM clients
- We are all responsible for preventing FWA & reporting suspected cases without fear of reprisal
FWA Training Purpose Cont’d

- Training will give you basic information necessary to understand what FWA is & what your obligations are if you suspect it is happening
- By knowing the basics of FWA, we are in compliance with CMS & MTM client requirements & help reduce potential for future FWA
- By looking out for FWA, we protect Federal funding given to Medicaid & Medicare programs for NEMT
FWA Training Topics

- FWA definitions
- Why MTM conducts FWA training
- Applicable Federal laws
- FWA obligations
- Examples of member FWA
  - What to do when member FWA is suspected
FWA Training Topics Cont’d

- Examples of First Tier, Downstream & Related Entity FWA
  - What to do to when First Tier, Downstream & Related Entity FWA is suspected
- Who is responsible for identifying FWA?
- Who is responsible for monitoring & auditing FWA at MTM?
- Preventing FWA
- Reporting FWA
- Protection for whistle blowers
FWA: What is Fraud?

- An intentional deception or misrepresentation made by a person with knowledge that deception could result in unauthorized benefit to himself or another person.
- Includes any act that constitutes fraud under applicable Federal & State law.
FWA: What is Waste?

- Overutilization of services or other practices that result in unnecessary costs.
- Generally not caused by criminally negligent actions but rather misuse of resources.
FWA: What is Abuse?

- Provider practices that are inconsistent with sound fiscal, business, or medical practices & result in:
  - Unnecessary cost to Medicaid/Medicare program
  - Reimbursement for unnecessary services or services that fail to meet professionally recognized standards for healthcare
- Includes covered member practices that result in unnecessary costs
FWA Training Importance

- MTM does business with Medicare & Medicaid clients
- Clients are required by CMS to conduct FWA training with First Tier, Downstream & Related Entities (subcontractors)
  - MTM must do the same with our First Tier, Downstream & Related Entities (transportation providers, drivers & office staff)
  - In short, because MTM clients are regulated by CMS, so is MTM & our subcontractors
- Documentation of annual FWA training must be maintained & available to CMS/clients when requested
FWA Training Requirements

- Applicable laws & regulations
  - Federal & State specific
- Obligations to have policies & procedures in place to address FWA
- Types of member FWA & possible resolutions
- Types of subcontractor FWA & possible resolutions
- Process for reporting suspected FWA
- Protections for employees who report FWA
FWA Laws & Regulations

- Suspected violations of:
  - False Claims Act; 31 U.S.C. §3729
  - Stark Law
  - AntiKickback Statute
- Suspected marketing violations, including inducements
- Acts defined in 18 U.S.C. Chapter 47, especially §1001 & §1035
- Health Insurance Portability & Accountability Act (HIPAA)
- State-specific laws & regulations that address Medicaid/Medicare FWA
FWA: Your Obligations

- Have policies & procedures in place
- Comply with all policies & procedures developed & amended by MTM relative to FWA
- Acknowledge that payments made to you consist of Federal & State funding
  - You can/will be held civilly/criminally liable for non-performance, misrepresentation or FWA of services rendered to MTM & its clients
- Immediately refer all suspected or confirmed FWA to MTM
Examples of Member FWA

- Changing, forging, or altering:
  - Prescriptions
  - Medical records
  - Referral forms
- Lending insurance card to another person
- Identity theft
- Using NEMT for non-medical services
- Misrepresenting eligibility status
- Resale of medications to others
- Medication stockpiling
- Doctor shopping
Resolution Options for Member FWA

- Add a note to member’s file advising MTM for future trips
- Add member’s name to a list of frequent abusers
  - Trip requests will be monitored & managed to prevent future FWA
- Report issue to designated State or County Medicaid office or MTM client
Examples of Provider FWA

- Falsifying credentials
- Billing for services not rendered
- Inappropriate billing
- Double billing, up-coding & unbundling
- Collusion among providers
  - Agreeing on minimum fees they will charge & accept
- Falsifying information submitted through prior authorization or other mechanism to justify coverage
Resolution Options for Provider FWA

- Recover trip cost
- Provide education
- Make recommendation for an audit of trip records
- Establish Corrective Action Plan (CAP)
- Disciplinary action
- Dismissal from MTM network of providers
Who is Responsible for Identifying FWA?

- MTM Employees
- Board of Directors
- Drivers
- Transportation Providers
- Office Staff
Who Monitors FWA at MTM?

- Cases reported to Quality Management department
- Compliance Auditor investigates each reported incident
  - Notes results of investigation in member’s file
- FWA reported against First Tier, Downstream, or Related Entities handled in the same manner
- MTM reports incidents of FWA to clients on monthly basis
Preventing FWA before it happens is critical.

First Tier, Downstream & Related Entities, as it relates to MTM riders, should report incidents of FWA they suspect to MTM’s Quality Management department ASAP.

Report all cases of suspected FWA to MTM immediately.
Preventing FWA

- MTM staff are diligent & watch carefully for signs of FWA
  - Deny a trip if it seems “suspect”
  - Push trip request up internal chain of command to Team Lead
  - Contact client & get their guidance
  - Report suspicious activity to Quality Management department for investigation
Reporting FWA

- Contact MTM’s Quality Management department
  - 1-866-436-0457
- Try to include all pertinent information:
  - Subject of FWA
  - Subject ID information
  - FWA description
  - Any other important information
FWA Reporting Protections

- Whistleblowers offered protection against retaliation under the False Claims Act
  - Employees discharged, demoted, harassed, or otherwise discriminated for reporting FWA or as a consequence of whistleblowing entitled to relief necessary to make employee whole
FWA Conclusion

- Training has given you:
  - Knowledge about what FWA is & why it is important to identify cases of suspected FWA
  - Tools necessary to feel confident in reporting suspected FWA without fear of reprisal
  - Understanding of why MTM requires training
  - Knowledge that everyone is responsible for reporting FWA
  - Knowledge that preventing FWA is critical—stop it before it happens
HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)
HIPAA Introduction

- Training will:
  - Provide information necessary to ensure member health information is regarded with privacy & security
  - Provide information necessary to meet standards for privacy & security set forth by governing agencies
  - Focus on daily functions of transportation providers to ensure member privacy & security
HIPAA Background

- Enacted by Congress in 1996
- Department of Health & Human Services (HHS) implemented final Privacy Rule on April 14, 2003
- Compliance date for Security Standards was April 20, 2005
- HITECH Act of 2009 widened scope of privacy & security protections available under HIPAA
HIPAA Privacy Rule

- Ensures nationwide uniform procedural protection for all health information
- Imposes restrictions on use & disclosure of Protected Health Information (PHI)
- Gives people greater access to medical records
- Provides people with more control over health information
HIPAA Security Rule

- Privacy Rule deals with PHI in general; Security Rule deals with electronic PHI (ePHI)
- Security Rule for ePHI greatly expanded in 2009 under American Recovery & Reinvestment Act
ARRA 2009

- HITECH Act of American Recovery & Reinvestment Act of 2009 (ARRA) imposes new obligations on a covered entity (CE) & business associate (BA)
  - Breach notification
  - BA directly responsible for compliance with Security Rule
  - BA liable for violations of Security Rule & breeches
HIPAA Expectations

- Use or disclose PHI only for work related purposes
- Limit use & disclosure to “minimum necessary” to accomplish intended purpose of use, disclosure, or request
- Exercise reasonable caution to protect PHI under your control
- Understand & follow MTM privacy policies
- Report privacy problems to supervisor & MTM ASAP
Protected Health Information (PHI)

- PHI is individually identifiable health information that is:
  - Transmitted by electronic media
  - Maintained in electronic media
  - Transmitted or maintained in any other form or medium

- When MTM member, agency, or health provider gives personal information to MTM, that information becomes PHI
Examples of PHI

- Any information that might connect health information to an individual

- Name or address
- SSN or other ID number
- Medicaid/Medicare number
- Physician notes
- Billing information
Use or Disclosure of PHI

- Privacy Rule covers use & disclosure of PHI
- Designed to minimize careless or unethical disclosure
- PHI can’t be used or disclosed unless it is permitted or required by the Privacy Rule
Use vs. Disclosure

- PHI is used when it is:
  - Shared
  - Examined
  - Applied
  - Analyzed

- PHI is disclosed when it is:
  - Released/ transferred
  - Accessed in any way by anyone outside entity holding information
Use or Disclosure of PHI

- PHI may be shared when it’s for “TPO”
  - **Treatment**: Management of healthcare & related services that includes coordination among healthcare providers
  - **Payment**: Various activities of healthcare providers to obtain payment or be reimbursed for services
  - **Healthcare Operations**: Certain administrative, financial, legal & quality improvement activities of covered entity necessary to run its business & to support core functions of Treatment & Payment
Use or Disclosure of PHI

- Transportation Providers permitted to use or disclose PHI for:
  - Scheduling trip information
  - Confirming special needs or adaptive equipment
  - Incidental use such as talking to a facility or medical provider
Minimum Necessary

- Use or disclosure of PHI should be limited to minimum amount of health-related information necessary to accomplish intended purpose of use or disclosure
- MTM has developed policies & procedures to make sure least amount of PHI is shared
- If you have no need to review PHI, then stop!
Maintaining Privacy: Written

- Keep information in a folder during business hours & locked drawer after hours
- Shred documents containing PHI after use
- Keep a minimal amount of information in hard copy format
- Do not leave documents unattended at printer or Xerox machines
Maintaining Privacy: Telephone

- Leave minimal information necessary on voice mail or answering machines regarding confirmation of trips, or ask member to return call to confirm
Maintaining Privacy: Faxes

- Always include a cover sheet that:
  - States it is a confidential document
  - Gives a contact if fax is received in error
  - Spells out HIPAA language
- Verify fax number before sending
Maintaining Privacy: Email

- Emails containing PHI must be sent securely
- Follow all directions for secured email
- Do not enter any PHI in subject line
Maintaining Privacy: Workstation/Vehicle

- Always lock access to computer with a password & use privacy notice
- Remove documents containing PHI from copiers & printers ASAP
- Keep PHI in a folder or upside down during working hours
- Remove PHI from desk or vehicle & place in locked drawer at end of work day
- Do not discuss PHI in public areas
Privacy Practices Designed to Protect PHI

- Verify identity & authority of requestor before releasing PHI
- Transmit PHI by telephone only when it can not be overheard
- When leaving messages, limit information left to member’s name, a request to return call & your name/telephone number
Misuse of PHI can result in civil & criminal sanctions:

- **Civil Penalties**: Up to $25,000/year for inadvertent violations; $250,000 for willful neglect; $1.5 million for repeated or uncorrected violations
- **Criminal Penalties**: Up to $250,000 fine & prison sentence up to 10 years for deliberate violations
- Sanctions by DHHS
- Other penalties related to not meeting contractual obligations
Examples of Misuse of PHI

- A South Dakota medical student took home copies of 125 patients’ psychiatric records to work on a research project
  - He disposed of material in dumpster of a fast food restaurant, where they were found by a newspaper reporter
- In Florida, several hundred hospital workers browsed records of famous patient who recently came to the facility, even though few of the workers were involved in the case
Reporting Misuse of PHI

- Report incidents of accidental or intentional disclosure to your supervisor & MTM
- No adverse action will be taken against anyone who reports in good faith violations or threatened violations of Privacy Rule, Security Rule or related policies
- MTM must report to DHSS all uses or disclosures not permitted by BA provisions of contract or HIPAA
Breach of ePHI

- HITECH Act imposes data breach notification requirements for unauthorized uses & disclosures of unsecured (unencrypted) PHI
- Breach is unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of information
Examples of Breach of ePHI

- Theft of 57 hard drives at an insurance company’s training facility, including images from computer screens containing data that was encoded but not encrypted
- Theft of laptop containing PHI that was password protected but not encrypted
Breach Notification

- Notice to individual of breach of his/her PHI is required under the ARRA HITECH Act
- Breaches involving PHI of more than 500 persons in one circumstance must be immediately reported to DHHS by covered entity
  - Will be posted on DHHS site
- BAs must report security breaches to covered entity
Enforcement of Privacy & Security

- Office of Civil Rights has enforced Privacy Rule since 2003
- CMS has enforced Security Rule since 2005
- As of July 27, 2009 DHHS has delegated enforcement of both rules to Office of Civil Rights
HIPAA Resources

- CMS
- Office of Civil Rights
  - www.hhs.gov/ocr/hippa/
- US DHHS
  - www.hhs.gov
HIPAA Glossary

- **Business Associate**: Person or entity that performs certain functions or activities that involve use or disclosure of PHI on behalf of, or provides services to a covered entity.

- **Protected Health Information**: Individually identifiable health information.

- **Minimum Necessary Information**: Current practice is that PHI should not be used or disclosed when not necessary to satisfy a purpose or carry out a function.