



**YOU GOT TO BE KIDDING:
HIPAA, MEDICARE AND
DOCUMENTATION**

ISN'T IT HARD ENOUGH



WHY IS IT SUCH A BIG DEAL??

- **Ex-Houston club owner admits EMS Medicare fraud**
- Between 2005 and 2010, Medicare records show that at least \$488 million was paid to non-emergency Harris County ambulance providers. By comparison, the Houston Fire Department received nearly \$54 million during that same time period for emergency ambulance transports.

WHY IS IT SUCH A BIG DEAL

- [Philadelphia Ambulance Fraud](#)
- OIG estimates that 25% of ambulance trips are not necessary
 - - resulting in over \$400 million in over payments

Medicare Compliance

- Compliance requires the involvement of every single person
 - It does not just relate to billing practices
 - Companies with the best of intentions often unintentionally commit compliance errors, which with more regularity are resulting in sanctions

Medicare Compliance Program

- Written documentation of policies
- Designated compliance officer
- Periodic compliance training
- Frequent audits of compliance risks and company compliance performance
- Timely correction of errors
- Enforced and consistent discipline for non-compliance
- Anonymous reporting mechanism
- Non-retaliation for reporting

Elements of Compliance

- * Our organization
 - * Provides a culture that encourages ethical conduct and a commitment to compliance with the law
 - * Exercises due diligence to prevent and detect both intentional criminal conduct and unintentional errors
 - * Performs risk assessments to identify areas of concern and diligently performs audits and monitoring
 - * Assures that the compliance program is reasonably designed, implemented and enforced

Elements of Compliance

- Effective Plan
 - Written policies and procedures
 - Designation of a compliance officer and committee
 - Education and training
 - Open lines of communication
 - Non-intimidation and Non-Retaliation
 - Enforcement of Disciplinary Standards
 - Auditing and Monitoring
 - Investigation, Response and Prevention of Fraud, Waste and Abuse

Understanding the Code of Conduct

- Commitment
 - Each employee represents and functions as an agent of the company. Therefore it is important that each person conducts themselves with absolute integrity at all times
- Purpose
 - Recognize the unique value of each person
 - Believe that every patient and co-worker should be treated with respect
 - Believe that our business should be conducted with absolute and unyielding integrity in accordance with all industry standards and government regulations

Fraud, Waste and Abuse

- Fraud
 - Any intentional act or omission designed to deceive patients or the government, resulting in the patients or government suffering a loss and or the perpetrator achieving a gain
 - Over billing
 - Billing for services not rendered
 - Falsifying documentation

Fraud, Waste and Abuse

- Waste
 - The careless expenditure, consumption, mismanagement or use of resources whether intentional or unintentional resulting in charge to patients or government

Fraud, Waste and Abuse

- Abuse
 - Intentional mistreatment of patients or destructive misuse or diversion of assets and resources and activities that are inconsistent with sound medical or professional practices

Compliance with Medicare and Medicaid

- Guidelines have been developed by both the OIG and OIGM outlining expectations
 - Adherence to guidelines for practice, treatment and billing
 - Detection processes for preventing fraud, waste and abuse
 - Strategies for complying with federal and state program requirements

Improper alterations to records

- Documentation
 - Must be an accurate record of actual care provided
 - Must not be altered to allow for billing changes
 - Must comply with the HIPAA and HITECH provisions
 - Signature from patient for services actually rendered

Proper documentation

- Medical Necessity
 - Patient was transported in an emergency situation such as an accident, injury or acute illness
 - Patient needed to be restrained
 - Patient was unconscious or in shock
 - Patient required oxygen or other emergency treatment
 - Patient exhibits signs and symptoms of acute respiratory or cardiac distress
 - Patient exhibits signs and symptoms suggesting a possible acute stroke
 - Patient had to remain immobile because of a fracture
 - Patient was experiencing severe hemorrhage
 - Patient could only be moved by stretcher
 - Patient was bed confined prior to transport

Documentation

- Risk assessment
- Employee certification
- Training
- Investigation and discipline
- Audits and monitoring

Documentation

- Purposes
 - Clinical Record
 - Legal Representation of services provided
 - Provide Data
 - Provide for financial reimbursement
 - Compliance

Documentation

- Protection for EMS personnel
- Reflection of good patient care

Standard of Care

- Standard of Care
 - The expected care, skill, & judgment under similar circumstances by a similarly trained, reasonable provider
- Negligence
 - Deviation from accepted or expected standards of care expected to protect from unreasonable risk of harm
- Elements Required to prove Negligence
 - Duty to Act
 - Breach of duty
 - Actual damage or harm
 - Proximate cause

Consent

- Issues Surrounding Consent
 - Patient has legal & mental capacity
 - Patient understands consequences
 - Types of Consent
 - Informed
 - Expressed
 - Implied
 - Involuntary
- Issues Surrounding Consent
 - Specific Consent Issues
 - Minors
 - Emancipated Minor
 - Prisoners

Refusal of Care

- Refusals
 - Consent for Transport vs. Treatment
 - Withdrawing Consent
 - Refusal of Service
 - Has legal & mental capacity
 - Is informed of risks & benefits
 - Offer alternatives
 - All of the above are well documented & witnessed
- Refusals
 - Incompetent Persons
 - Unable to understand the nature & consequences of his/her injury/illness
 - Unable to make rational decisions regarding medical care due to physical or mental conditions
 - Do not assume incompetence unless obvious

DOCUMENTATION

An accurate, complete, legible medical record implies accurate, complete, organized assessment and management

Documentation

- Characteristics of good medical record
 - Accurate
 - Complete
 - Legible
 - Free of extraneous information

Accurate

- Document facts, observations only
- Do NOT speculate about patient or incident
- Double-check numerical entries
- Recheck spellings of:
 - Persons
 - Locations
 - Medical terms

Complete

- Include all requested information
- If information requested does not apply, note "not applicable" or "N/A"
- Include at least two sets of vital signs on every patient
- Failure to document implies failure to consider
- If you look for something and it isn't there, document its absence

COMPLETE

IF IT ISN'T DOCUMENTED,
IT WASN'T DONE!

Legible

- If you cannot read the report, you may be unable to determine what happened
- Documents presented in court must "speak for themselves"
- If a document cannot be deciphered, the jury has to right to ignore it altogether

LEGIBLE

If the report is sloppy, others will assume that the care was equally sloppy

Free of Extraneous Information

- Avoid labeling patients ("drunk", "psych patient")
- Describe the observations you made
- Preface comments made by the patient with "per the patient" or "patient stated"

Free of Extraneous Information

- Record hearsay only if applicable
- Do **NOT** record hearsay as facts
- Use quotation marks only if a statement is accurate word-for-word

Documentation

- A copy of the report must be left with the patient at the receiving hospital
 - State law requires this
 - Patient care has not legally been transferred until the hospital has your written report

Documentation

- The person who rode with the patient writes the report
- All personnel who participated in care should review the report

Documentation

- If something needs to be corrected, correct it
- The sooner an error is corrected, the more credible and reliable the change is
- Mark through information so it is still readable
- Then write in the new information and initial/date the change

Documentation

- Be sure treatments recorded match the mechanism of injury or the diagnostic impression
- If something should have been done that was not, state why

HIPAA Compliance

- HIPAA – The Health Insurance Portability and Accountability Act
 - Enacted in 1996
 - Main focus on Insurance practices
 - Three pertinent provisions for EMS
 - Electronic transactions and code sets (TaCS)
 - Security of PHI
 - Privacy
 - All agencies involved in using information required to be compliant by April 14, 2003

HIPAA Compliance

- Privacy
 - Required compliance by April 14, 2003
 - Regulates the uses and disclosures of protected health information (PHI)
- Security
 - Required compliance 2005
 - Has many common intersections with the Privacy portion

HIPAA Compliance

- PHI – Protected Health Information
 - Individually identifiable or demographic information
 - Regarding past, present or future physical or mental health or the provision of care to an individual
 - Created by or received by a health care provider
 - Oral or recorded in any form

HIPAA Compliance

- Examples of PHI Identifiers
 - Name
 - Geographic identifiers smaller than a state
 - Dates
 - Phone/fax numbers
 - E-mail addresses
 - Medical record numbers
 - Certificate/license numbers
 - Health plan numbers

HIPAA Compliance

- The Privacy Rule identifies
 - Covered Entities (Health Care Providers) must protect and limit access to PHI based on roles
 - Means we must create policy and procedure that identifies
 - The types of persons that need access to PHI
 - The specific PHI that they need access to
 - How unauthorized persons will be limited access

HIPAA Compliance

- How do I know
 - Gap Analysis
 - All agencies must go through the exercise
 - Identify how PHI is created
 - Identify how it flows through the organization
 - Identify who has access at each step
 - Internal
 - External (Business Associate)

HIPAA Compliance

- Where does the information go
 - Identify information
 - Oral
 - Written
 - Electronic
 - To other providers
 - On scene
 - At the destination

HIPAA Compliance

- Internal
 - Record keeping
 - QA
 - Storage
- External
 - QA
 - Billing
 - Storage

HIPAA Compliance

- Roles and Responsibilities
 - HIPAA should not interfere with the provision of patient care
 - Who needs to have access to patient information
 - Medic
 - Driver
 - Dispatcher
 - Administration
 - Billing

HIPAA Compliance

- What information needs to be accessed
 - Based on role and responsibility
 - May be different for every organization
 - Must be clearly identified in Policy and Procedure
 - Everyone is accountable for protecting PHI

HIPAA Compliance

- Other Policy and Procedures
 - Develop a contingency plan to respond to disasters and ensure accountability and availability of PHI
 - Conduct audits of information system activity
 - Ensure that PHI has not been altered or destroyed
 - Have a formal process for ending association with the organization
 - Evaluate security measures
 - Have a formal process and contracts in place for relationships with business associates.
 - Means of accounting for release of PHI

HIPAA Compliance

- Help I'm Drowning
 - Appoint a Privacy Officer
 - Continually monitors systems and policies to insure that disclosure does not occur
 - Help to write and update policies
 - Review contracts
- Review
 - Identify
 - Prevent
 - Document
 - Evaluate

HIPAA Compliance

- Once we have identified what PHI is and how it flows
 - Write Policy and Procedures
 - Train Everybody on the accountability
 - Document...

HIPAA Compliance

- HIPAA provides for the safeguarding of PHI
 - We are required to inform all patients of our HIPAA compliance
 - Notice of Privacy Practices
 - Acknowledgement of receipt
 - If a patient cannot sign, documentation as to why (altered mental status) must be provided
 - Some documentation as to how the information will be given should also be given

HIPAA Compliance

- Individual rights
 - An individual may request their PHI at any time
 - Also should comply with State regulation
 - Individuals have the right to receive an accounting of disclosures of PHI by a CE in the six years prior to the date of request.
 - Need to keep a log of all disclosures

HIPAA Compliance

- Security
 - How do you protect against unauthorized access
 - Electronic
 - Paper
 - Radios

HIPAA Compliance

- Along with many other changes HIPAA must be incorporated into our daily practices.
 - Take all precautions to limit disclosure
 - Keep good records
 - Follow written policy and procedures
 - Inform patients
 - Stay up to date

HIPAA Compliance

- New Requirements 2009
 - Breach Notification Rules
 - Updated requirements for Business Associates
 - Enhanced Individual Privacy Rights
 - Increased Enforcement and Penalties

2009 Updates Breach Notification

- Covered Entities are required to notify affected individuals of a breach of privacy or security of his/her PHI
 - Applies to only unsecured PHI
 - Secured is encrypted or destroyed
 - Encryption requirements complex

2009 Update

- What is a Breach
 - Impermissible acquisition, access, use or disclosure of PHI which "compromises security or privacy of PHI"

Breach Assessment

- Identify who used PHI or who it was disclosed to
- Were immediate steps taken to mitigate harm
- What type and amount of PHI was involved

2009 Tips

- Know where you maintain PHI in your organization
 - Understand what constitutes a breach
 - Conduct a risk assessment
 - Develop detection system and process

Business Associate Agreement

- New stronger wording for Business Associates
 - Now have some responsibility for compliance on their own
 - Must employ certain safeguards

Other Requirements

- Uses or disclosures of PHI that involve more than the minimum necessary may qualify as a breach
- Individuals have a right to upon request:
 - Expanded accounting of all disclosures
 - Access and copies of PHI in electronic format at cost.

New Enforcement

- No more emphasis on voluntary compliance or only complaint – driven approach.
 - Focused audits by more agencies
 - Significant civil penalties
 - Authority to state attorneys to bring civil actions
 - \$1,000 penalty for reasonable cause
 - \$10,000 - \$50,000 if willful neglect
 - Whistleblower rights
