# Healthcare Fraud and Compliance

**Presentation prepared for:**
**Northeast Ohio HFMA**
**Healthcare Huddle**
**November 18, 2016**

# Presentation Overview

- Overview of an effective Compliance Plan
- False Claims Act
- Training and Education Requirements
- Common Mistakes and Fraud Schemes

# What is a Compliance Program?

- A Compliance Program is a centralized process to identify and prevent illegal conduct, and to promote honest, ethical behavior in the day-to-day operations of an organization.
- The Department of Health & Human Services (HHS) sets the rules and oversees the Center for Medicare & Medicaid Services (CMS) & the Office of Inspector General (OIG).
- The rules can be found under the *Federal Sentencing Guidelines*.

# OIG Recommended Compliance Program Elements

Compliance Program Elements:

1. Adopt appropriate **Policies & Procedures**
2. Designate a **Compliance Officer/Committee**
3. Conduct Internal **Monitoring & Auditing**
4. Conduct **Training & Education**
5. **Respond** to detected errors
6. **Enforce** disciplinary standards
7. Develop **open lines of communication**

# What are the Benefits of a Compliance Program?

- Helps fulfill an organization's mission, vision, and values.
- Assists in identifying weaknesses in internal systems and management.
- Improves patient care and fulfills legal duties to comply with applicable laws.
- Demonstrates strong commitment to honest and responsible provider and corporate conduct.
- Identifies and prevents criminal and unethical conduct.
- Encourages employees to report potential problems.
- Develops procedures that allow a prompt, thorough investigation of alleged misconduct.
- Initiates immediate and appropriate corrective action.
- Through early detection and reporting, minimizes the loss to the government from false claims and thereby reduces an organization's exposure to civil damages and penalties, criminal sanctions, and administrative remedies.

# Federal Requirements for Compliance Plans

- Section 6401 of ACA – All providers that participate in Medicare, Medicaid and CHIP must have a compliance program that meets the core elements of the OIG guidelines.
- Entities must provide information specific to Federal False Claims Act, Whistle Blowers Protection and applicable State Laws.
- **Whistleblower Protection**: the organization will NOT retaliate against any individual who alerts the organization to ongoing fraud/abuse against the government or any other conduct in violation of the organization's Compliance Program.

# The False Claims Act

- Information
  - Deals with fraud and abuse in billing and claims submission
  - All claims submitted must be: true, complete & accurate
  - False means wholly or partially untrue
  - Must have "intent" –
    - actual knowledge,
    - deliberate ignorance, or
    - reckless disregard that the claim is false.

- Penalties
  - There are civil and criminal penalties
  - $5,500 - $11,000 per each false claim + 3x the value of the claim
  - Implement a Corporate Integrity Agreement (CIA) – 5 yr term
  - Exclusion from Medicare, Medicaid & any governmental program (Anywhere from 6 months to permanently)
  - Statue of Limitation: In some instance, application of the law up to 10 years

# Duty to Refund Overpayments

- ACA includes a provision that providers must disclose and return any overpayments that result from mistaken or erroneous claims.
  - Final Rule issued February 12, 2016
  - 6 years after statute passed
  - 4 years after Proposed Rule published
- Key Takeaways:
  - Applies to Medicare Parts A and B (Medicare Parts C and D are covered under a separate proposed rule; no rule for Medicaid)
  - 6 year lookback period
  - 60 days begins once the overpayment is "identified"
    - 6 month investigation or due diligence period

# Billing and Claim Submission Requirements

- All billings must reflect truth and accuracy.
- All medical record documentation must be complete, accurate, and support the service being billed.
- Only bill for items or services that are actually rendered.
- Only bill for services that are reasonable and necessary for the diagnosis or treatment of the patient's illness or injury. (Must be supported by medical record documentation.)
- Properly code claims to actually reflect the service furnished to the patient consistent with the patient's diagnosis.
- Avoid duplicate billing for the same services.

*Preparation and submission of claims or other requests for payment from federal and state health care programs is the* ***biggest single risk area for providers****.*

# Common Billing Mistakes

- Inaccurate or incorrect coding
- Upcoding
- Unbundling of services
- Billing for medically unnecessary services, or other services not covered by the relevant health care program
- Billing for services not provided
- Duplicate billing
- Insufficient documentation
- False or fraudulent cost reports

# Most Common Types of Healthcare Fraud

- Billing for services not rendered.
- Billing for non-covered services as a covered service.
- Mispresenting dates of service.
- Misrepresenting locations of service.
- Misrepresenting provider of service.
- Waiving of deductibles and/or co-payments.
- Incorrect reporting of diagnoses or procedures and unbundling of services.
- Overutilization of services.
- Corruption (kickbacks and bribes).
- False or unnecessary issuance of prescription drugs.

*See* CMS Fact Sheet *available at* https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/fwa-factsheet.pdf.

# Education and Training

- Compliance has two components:
  - Health care fraud and abuse
  - General CMS compliance
- Providers enrolled in Medicare Part A or B are "deemed" to have satisfied the fraud and abuse portion of this required training **if they provide their own fraud and abuse training to employees** (they must document this training if not using the CMS training materials).
- Training is required annually for all providers who contract with and are paid by Medicare Advantage organizations or Medicare Part D drug plans for services rendered to Medicare Part C and D beneficiaries
  - Providers that contract with a MA plan or part D plan (first-tier, downstream, or related entities, or "FDRs") complete this compliance requirement by completing the CMS training on fraud and abuse and providing a certificate of completion to the organization/plan.

# Compliance Education and Training

- Sales and marketing;
- Utilization management;
- Quality improvement;
- Applications processing;
- Enrollment, disenrollment, membership functions;
- Claims administration, processing and coverage adjudication;
- Appeals and grievances;
- Licensing and credentialing;
- Pharmacy benefit management;
- Hotline operations; Customer service;
- Bid preparation;
- Outbound enrollment verification;
- Provider network management;
- Processing of pharmacy claims at the point of sale;
- Negotiation with prescription drug manufacturers and others for rebates, discounts or other price concessions on prescription drugs;
- Administration and tracking of enrollees' drug benefits, including TrOOP balance processing;
- Coordination with other benefit programs such as Medicaid, state pharmaceutical assistance or other insurance programs;
- Entities that generate claims data; and
- Health care services.

# FCA Facts

- Since 2009, the Dept. of Justice has recovered more than $26.5 billion through False Claims Act cases.
  - More than $16.7 billion was recovered from the healthcare industry alone.
- In 2015, the Dept. of Justice recovered more than $3.5 billion in settlements and judgments from False Claims Act cases.
  - Over half of this amount, $1.9 billion was recovered from companies and individuals in the healthcare industry.
- In 2015, most False Claims actions were filed by whistleblowers in *qui tam* actions.
  - *Qui Tam* actions allow individuals to file lawsuits alleging false claims on behalf of the government.
  - If the government prevails, the whistleblower receives up to 30% of the recovery. There is a major incentive for whistleblowers, especially current and former employees, to come forward with qui tam actions.
    - In 2015, approximately 85% of FCA actions were initiated by whistleblowers.

# FCA Facts

- In September, 2015 the DOG released a Memo indicating indicated that the DOJ would begin focusing on individual wrongdoers as well, holding them personally liable.
  - Areas of concern/high investigation:
    - Physician Compensation (Violations of Stark / Anti-Kickback Statutes)
    - 60 Day Deadline to Return Discovered Overpayments
    - Enforcement of Federal Grant Limitations
    - Enforcement of Overpayments for Medically Unnecessary Services / Failure to Follow NCDs and LCDs
    - Billing for Services Never Provided
    - Improper Delegation/Supervision

# 5 False Claims Act Trends

- Major issues surrounding FCA that emerged in 2015 included:
  - **Extrapolation**: several government rulings in favor of extrapolation have essentially lowered the government's burden in proving wider-scale fraud.
  - **Focus on Physician Compensation**: Several settlements focused on compensation arrangements that improperly took into account the value of physicians' referrals or paid physicians for services not performed (Medical Director relationships, downstream revenue, etc.).
  - **Focus on Individual Liability**: Increase in the number of ***individuals*** being held accountable for fraud – not just the organizations they work for. One key change is that to be eligible for any cooperation credit, companies must give up the individuals involved in the fraud, no matter where they sit within the company.
  - **Disclosure of Overpayments**: Enforcement of provider duty to report overpayments within 60 days of discovering the overpayment.
  - **Recognition of Implied Certification**: Enforcement of implied certification allows a whistleblower to bring a qui tam action based on statutes or regulations outside the FCA. Under this theory, the government or a whistle-blower can allege a claim submitted by a provider is false if they can show the provider billed for services in violation of some Medicare rule or regulation.

# Stark Law Overview

- The Stark law prohibits a provider from submitting any claims for a "designated health service" (DHS) if the referral of the DHS comes from a physician with whom the provider has a prohibited financial relationship.
  - Applies to all contracts between a hospital and physicians who refer business to the hospital.
  - All contracts with physicians should be referred to legal counsel for review.
  - No claims for payment should be submitted pursuant to a contract that violates the Stark Law.
- An exception under the Stark law must be met in order to allow the financial relationship between the parties.

# Relationships That Must Comply with the Stark Law

- **Employment agreements with physicians**
- **Recruitment agreements with physicians**
- **Medical director and other administrative agreements with physicians**
- **Lease agreements with physicians**

Remember: Stark Law is a **STRICT LIABILITY STATUTE**. In order to avoid Stark Law penalties, entities must ensure that ALL requirements are fulfilled for each individual exception.

# Anti-Kickback Statute

- The anti-kickback statute prohibits, in the health care industry, some practices that are common in other business sectors, such as offering gifts to reward past or potential referrals.

- The anti-kickback statute is a criminal prohibition against payment (in any form, whether payment is direct or indirect) made purposefully to induce or reward the referral or generation of federal and state health care program business.

  - Do not pay for referrals.
  - Do not accept payment for referrals that we make.
  - Always pay fair market value for services provided by referral sources. Any relationship with a referral source, such as a physician, should be reviewed by legal counsel.

# Anti-Kickback Statute

- Unlike the Stark law, the anti-kickback statute is an intent-based statute.

- The general rule of thumb is that any remuneration flowing between hospitals and physicians must be at fair market value for actual and necessary items furnished or services rendered based upon an arm's-length transaction and should not take into account, directly or indirectly, the value or volume of any past or future referrals or other business generated between the parties.

- It is a best practice to ensure that if physicians are being compensated for time (e.g. medical directorships, management agreements), the time spent and services being performed should be documented.

# Physician Compensation Fraud Alert

- OIG Fraud Alert Notice dated June 9, 2015
- Increase in investigations into physician compensation arrangements
  - Cites recent settlements with 12 individual physicians who entered into questionable medical directorship and office staff arrangements
- Physicians and hospitals must ensure that compensation arrangements reflect FMV for services actually performed
- May violate the Anti-Kickback Statute if even one purpose of the arrangement is for past or future referrals.
- Proper analysis of all physician compensation arrangements can help avoid OIG investigations and anti-kickback accusations.

# Trends in FCA Enforcement - Illegal Physician Compensation (Anti-Kickback and Stark Violations)

- ***Broward Health – Ft. Lauderdale, Florida***
  - Broward Health allegedly compensated at least nine employed physicians at rates above the fair market value and based compensation on patient referrals.
  - The rate was determined based on the physician's ability to increase patient referrals to the hospital system, in violation of Stark and Anti-Kickback Statutes.
  - Whistleblower alleged that Broward Health tracked the value of physician referrals and pressured physicians to increase referral volume when the referrals fell short of targeted goals.
  - Broward Health settled the case for approximately $70 million for violations of Stark and Anti-Kickback Statutes.
  - The lawsuit fell under the False Claims Act because federal law prohibits reimbursement from Medicare for services provided to patients that were illegally referred.

# Trends in FCA Enforcement - Illegal Physician Compensation (Anti-Kickback and Stark Violations)

- ***Adventist Health System – Altamonte Springs, Florida***
  - Adventist Health System allegedly paid bonuses to physicians based on the number of patients referred to Adventist Health System owned facilities.
  - The Health System encouraged doctors to purchase practices in certain areas in order to control referrals in specifically defined geographic areas.
  - A former physician was the whistleblower.
  - The Health System agreed to settle for $118.7 million
  - The lawsuit fell under the False Claims Act statute because federal law prohibits reimbursement from Medicare for services provided to patients that were illegally referred.

# Trends in FCA Enforcement - Illegal Physician Compensation (Anti-Kickback and Stark Violations)

- ***DaVita Healthcare Partners, Inc. – Denver, Colorado***
  - DaVita allegedly paid kickbacks to physicians to induce patient referrals to its dialysis clinics, which are located in 46 states.
  - DaVita then improperly billed for services rendered to the patients that were illegally referred, in violation of the FCA.
  - DaVita settled for $450 million.

- ***Daiichi Sankyo, Inc. – New Jersey***
  - Daiichi is a pharmaceutical company located in New Jersey that allegedly paid physicians to induce them to prescribe Daiichi drugs.
  - Medicare specifically prohibits reimbursement for drugs involved in kickback schemes, for this reason, Daiichi violated the False Claims Act.
  - Furthermore, it should be noted that if any physicians knowingly accepted the kickbacks, they may also be in violation of the False Claims Act.
  - Daiichi settled the False Claims Act violations for $39 million.

# Trends in FCA Enforcement - Violations of 60 Day Deadline to Return Overpayments

- ***Continuum Health Partners – New York, New York***
  - Whistleblower provided Continuum Health Partners with a list of over 900 billing claims that were submitted to Medicare in error.
  - It took Continuum Health Partners over 2 years after being alerted to the billings to return the overpayment.
  - Whistleblower then filed a *qui tam* action under the False Claims Act for Continuum's failure to timely return the identified overpayment.
  - Court ruled that Continuum had a duty to report and return the wrongly collected money from the time that the Whistleblower identified claims that were likely to contain overpayments.
  - The case has yet to settle, but early estimates indicate that it will settle for at least $2-3 million, which is based on the $1 million overpayment.

# Trends in FCA Enforcement - Improper Delegation / Supervision

- ***Adventist Health System - Altamonte Springs, Florida***
  - Adventist allegedly billed for and received reimbursement for radiation oncology services provided to Medicare patients without the required supervision of a qualified medical professional, as required by Medicare.
  - A former radiation oncologist for Adventist filed the *qui tam* action.
  - Because the procedures were not properly billed because of the lack of required supervision, Adventist violated the False Claims Act.
  - Adventist agreed to settle for $5.4 million, and the whistleblower will receive approximately $1 million.

# Trends in HIPAA Enforcement

- On September 29, 2015, OCR announced that it will begin Phase 2 of the HIPAA audits in early 2016.
- Phase 2 audits will include a combination of desk audits and on-site audits, will involve both covered entities **and business associates**, and will target specific common areas of noncompliance.
- With Phase 2 desk audits, covered entities and business associates will have two weeks to upload applicable HIPAA policies and procedures to a portal for OCR auditors to review.
- This remote audit approach will not allow for additional clarifications or discussion between the auditor and entity; therefore, policies and procedures must be accurate and complete and ready to upload.

# Lessons Learned from Recent HIPAA Enforcement Actions

- **Encrypt! Encrypt! Encrypt!** Although encryption is not a mandatory specification in the HIPAA Security Rule, encryption can greatly mitigate the potential risks that result from theft or loss of a portable device. OCR has repeatedly noted the importance of applying encryption whenever possible.
- **Risk Analyses**: Conduct on-going risk analyses of systems, networks, equipment and other repositories or access points to ePHI. Implement remediation plans and update policies and procedures to address critical risks identified during such risk analyses.
- **Device Management**: Don't sell, retire or reissue computers, portable devices, or even leased copiers or scanners without securely wiping all content. Implement appropriate policies and controls around mobile devices, particularly personal mobile devices used for work.

# Lessons Learned from Recent HIPAA Enforcement Actions

- **Hard-Copy PHI**: Do not underestimate or forget the security threats to non-electronic PHI and the associated requirements. Maintain policies and procedures to implement Privacy Rule requirements and to control the security and disposal of hard copy PHI.
- **Training**: Train employees and monitor adherence to HIPAA policies and procedures, including permissible uses and disclosures and incident reporting. In addition, educate employees with a general understanding of the threats and vulnerabilities to PHI and other sensitive data staff may access or handle.
  - All workforce members must receive training – employees, students, volunteers, medical staff, etc.
- **Incident Response**: Develop and test an incident response plan to quickly identify and mitigate potential security incidents.
- **Audit Preparedness**: Conduct gap analysis of current policies with Privacy and Security Rules; update risk analysis to ID threats and vulnerabilities, review business associate agreements; familiarize senior leadership with HIPAA compliance program.

# Examples of Recent HIPAA Violations

- HIPAA violations can create personal liability:
  - HHS investigated the University of Cincinnati Medical Center after an employee accessed the billing records of a patient with a STD and then shared the STD diagnosis with another individual who deliberately and maliciously posted the patient's STD diagnosis on Facebook. The patient sued the hospital, the employee, and the individual who subsequently posted the diagnosis. The case against the individuals was allowed to go forward.
  - A Walgreens pharmacist accessed her current boyfriend's ex-girlfriend's prescription records to obtain information on the ex-girlfriend's prescriptions for birth control and a STD and shared the information with her boyfriend and 3 other people. The ex-girlfriend sued Walgreens and the pharmacist, and a jury found them both liable for $1.4 million in damages to the ex-girlfriend.
  - A LPN was criminally convicted of violating HIPAA after she accessed a patient's medical information, shared it with her husband, and her husband called the patient and told the patient that he was going to use the information against the patient in an upcoming legal proceeding. The LPN was sentenced to 2 years of probation and 100 hours of community service, but she could have faced up to 10 years in prison and a fine of up to $250,000.00.

# Examples of Recent HIPAA Violations

- Merely snooping in a patient's medical record without permission creates HIPAA liability:
  - UCLA Health System paid $865,000 to settle potential HIPAA violations with the department of Health and Human Services after two celebrity patients filed complaints that UCLA Health System employees were looking at those celebrities' EMRs without a permissible reason.
  - A physician in Vermont was criminally convicted of a HIPAA violation after he looked at the medical records of women with whom he had a personal relationship.
  - Six employees of Cedars-Sinai Medical Center were fired for committing HIPAA violations when they accessed the records of patients they were not treating.
  - A hospital supervisor was disciplined for a HIPAA violation after the supervisor accessed, examined, and disclosed information from one of the supervisor's employees' medical record without the employee's authorization.

# HIPAA and Social Media

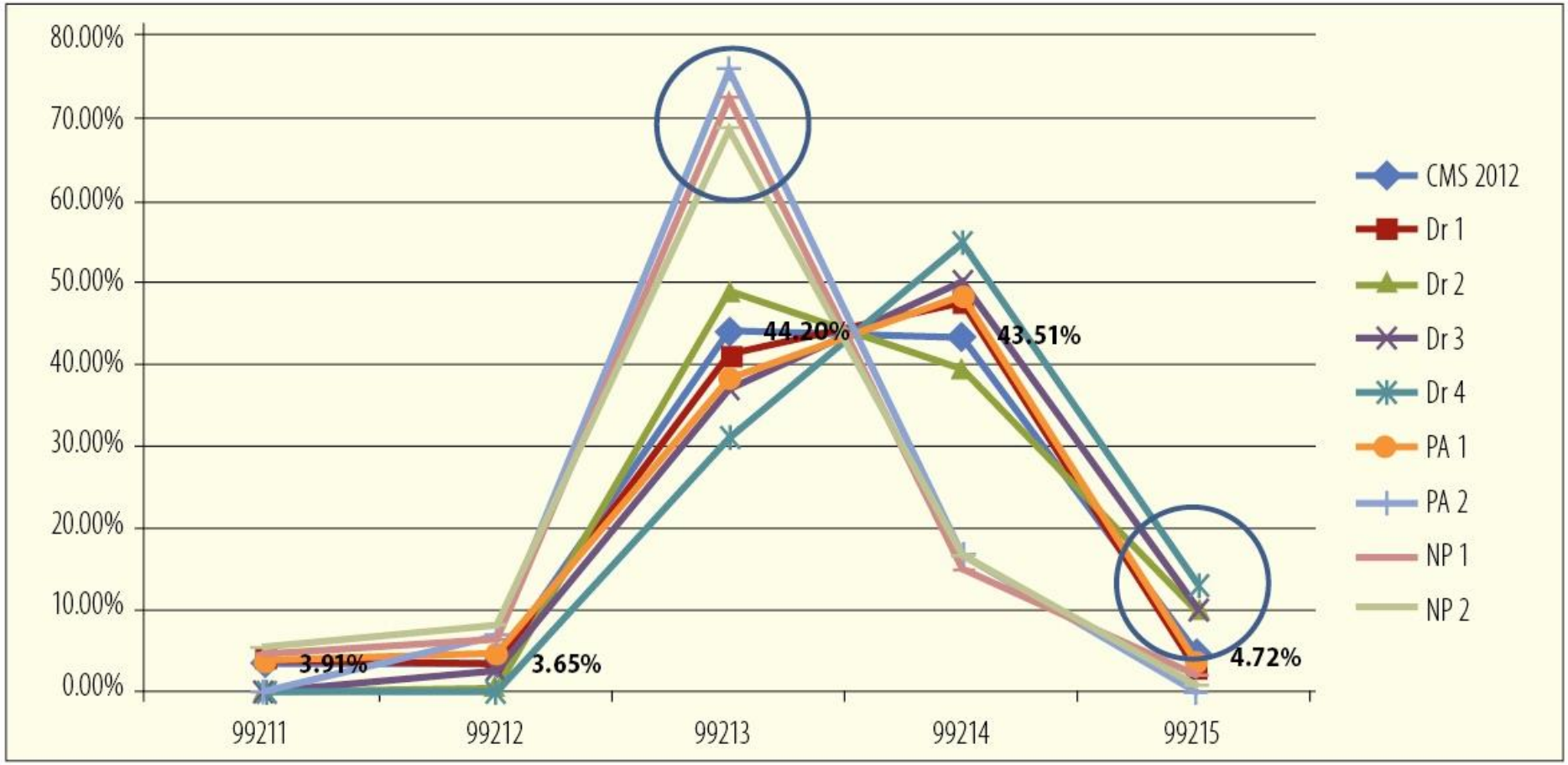
- Healthcare's unique challenges when it comes to Social Media
  - Privacy
  - Practice of Medicine Issues
  - Ethics in Becoming "Friends" with Patients
- Importance of developing a strong social media policy that balances risks and benefits of #hcsm
  - There is no "one size fits all" approach
  - Focus on managing, rather than controlling, your social media presence
  - Education and awareness are critical

# Examples

# You Can't Un-ring the Bell

- Client bills 99213 for all services

**Chart B:** Internal Medicine Practice Established Patient E/M Medicare Utilization vs CMS 2012 National Distribution



# There's no Place Like Home (Health)

**Case #1:`**

- Physician office becomes subject of DOJ investigation
- MA forging home health prescriptions for home health agency owned by father and husband

**Case #2:**

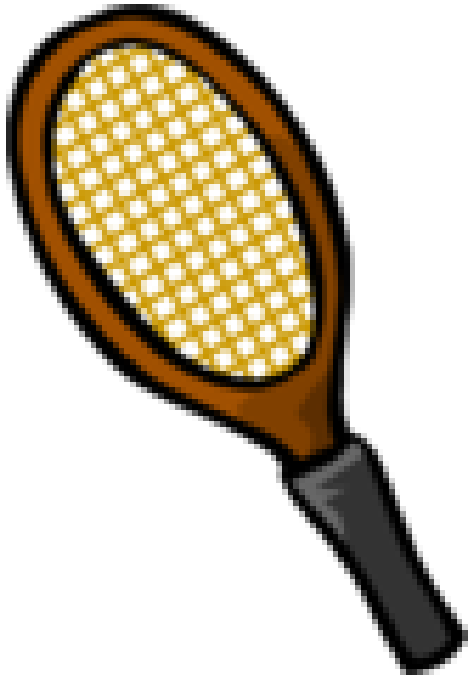
- Surgical assist at ASC provided home health care services to mother
- Both were indicted for Medicaid fraud, surgical assist on Medicaid exclusion list
- ASC was not checking exclusion list

# Balancing the Books – An Unbalanced approach

- Physician partnership (50/50)
- One physician out on maternity leave
- Practice continues to bill services equally under both physicians' NPIs for accounting purposes
- Physician never returns from maternity leave
- Remaining physician sues for reimbursement of overhead expenses
- Improper billing discovered and refunded to MAC
- Former partner files *qui tam*; remaining partner must settle Medicare and Medicaid funds with FCA damages

# Rehab Racket

- Question as to whether PM&R physician was physically seeing patients when initially admitted to rehab facility
  - H&P
  - Discharge instructions
  - Plan of care
- Investigation
  - Medical group
  - Hospital
  - SNFs and Rehab Facilities
- Self-disclosure
- Termination
  - Non-compete
  - Non-solicitation
- Report to licensing Board



# The Devil's in the Details

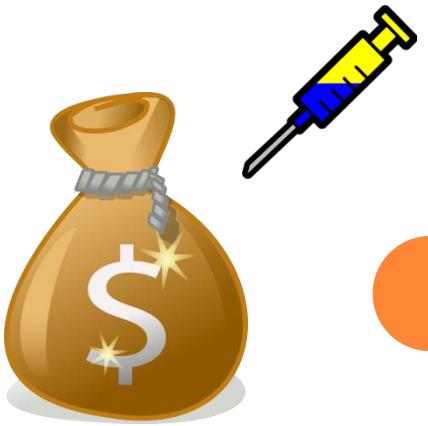
- LTACH leases 2 licensed surgery centers
- LTACH is not credentialed to provide surgical services
- LTACH's managed care contract pays outpatient services at 50% of billed charges, but industry standard is to attach an ASC fee schedule for surgical services
- LTACH does not update credentialing information
- LTACH does not add the 2 surgery center locations to its payor contracts

# Pass-Thru Billing

- Lab company performs the ordered tests; stamps hospital name on medical records
- Tests are billed under hospital's more lucrative payor contract
- No contractual arrangement between the lab company and hospital except for billing services

# Unspecified or Unclassified Codes – Unnecessary Consequences

- Using J3490 for Marlido Kits
  - Anesthetic injections are bundled into the injection procedure code (lidocaine, Marcaine, etc.)
  - Only therapeutic injections are separately billable
  - Injectable cannot be homeopathic (Traumeel, Sarapin etc.)
- Bariatric surgery codes
  - Using 43659 for bundled services and other bariatric surgeries
- Unbundling codes
  - Chiro and PT claims



# Waiving Co-Pays and Deductibles

**Case #1:**

- Provider waived co-pays and deductibles for all local police and fire departments
  - Competitor filed complaint

**Case #2:**

- Provider bundled all non-covered and covered services self-pay portions into one bill
- Provider then discounted the bill in the amount of the co-pay or deductible
- Patient account was deemed “paid in full”

# Overutilization and Unnecessary Services

- Joint Injections
- Nerve Conduction Studies
- Jacksonville, Florida - $10 million settlement
  - Physicians prescribed topical pain cream
  - Billed by compounding pharmacy owned by referring physicians
  - Estimated $2 billion in claims to Tricare since 2013

# Self-Prescribing

- Pediatrician prescribing for friends and family
- Urgent care physician prescribing for friends and family

# Key Takeaways

- Ensure your compliance plan is up-to-date
- Appoint Compliance Officer
  - Have a written chain of command
- Perform regular training and education
  - Ensure that the training includes real examples
  - Ensure that the training is interactive
- Promote constant communication
  - Have a formal reporting process for employees and leadership
  - Have an anonymous reporting process
- Investigate all reports
- Perform self-audits and evaluations
  - Ask Questions!!!!

# QUESTIONS?

Amanda L. Waesch, Esq.
**Brennan, Manna & Diamond, LLC**
75 East Market Street
Akron, Ohio 44308
330-253-9185
alwaesch@bmdllc.com

BRENNAN, MANNA & DIAMOND
ATTORNEYS & COUNSELORS AT LAW