They'll Never Investigate ME
RAC AUDITS, HIPAA DATA BREACHES...& DOCTORS

D. Scott Jones, CHC
Richard E. Moses, D.O., J.D.

INTRODUCTION
- How Doctors Think
- Quality of Care Investigations: OIG/DOJ
- HIPAA Breaches
- RACs & Post Payment Audits
- Conclusions

HOW DOCTORS THINK 101
Pressure on Private Practice

- Physician reimbursement declined 25% 1995-2008
  - *JAMA* 2010;303:747-753
- Patient Protection and Affordable Care Act (PPACA 2010) amended by the Health Care and Education Affordability Reconciliation Act (HCERA 2012)
  - 21.3% scheduled reduction in Medicare physician pay (postponed by the Continuing Extension Act of 2010)
  - Quality and Cost Payment (Section 3007) – Adjusts physician payments based on quality and cost through a value-based modifier, beginning January 1, 2015
  - PQRI – possible penalties for not reporting in 2015

Pressure on Private Practice

- Legally limited ability of independent practices to jointly negotiate for higher fees from payors
- Anti-Kickback Statute and Stark Law restrictions on ancillary services ownership and referrals
- Increased regulatory pressure: RAC Audits, HIPAA requirements, CMS and OIG investigations, OSHA
- Demand for a highly efficient business model with carefully managed overhead costs

Pressure on Private Practice

Changing Landscape

- 32 Million Americans may acquire new health insurance with the Patient Protection and Affordable Care Act ("PPACA")
- Increase from 260.2 Million Americans with health insurance to 292.6 Million under PPACA
- U.S. Physician workload anticipated to increase by 29% from 2005-2025
- Almost 50% of physicians are health system employees
How Doctors Think

• I got into medicine to take care of patients, not push paper or computer buttons.
• I’m not going to spend half my life learning to be a doctor just to bilk Medicare out of a few bucks.
• Somebody should take care of this technical stuff and let me get back to my patients.
• I order and use only the resources necessary to get the best outcome for my patients.
• Why would they investigate me? I’m a good doctor.

QUALITY OF CARE INVESTIGATIONS: OIG/DOJ

Compliance and Quality Investigations
St. Joseph’s Medical Center, Towson MD

- Based on a qui tam report, Dr. Mark Midei was accused of unnecessary cardiac stent placement
- An OIG investigation of stent placement triggered hospital investigations and a US Senate investigation
- Dr. Midei was accused of 585 unnecessary stent procedures in his last two years of practice
- Letters were sent to all patients advising them they may have a stent that was “Medically unnecessary”
- $22 Million settlement with DOJ, alleged violations of Anti-Kickback and Stark Law
- Hundreds of medical malpractice claims are filed by attorneys who obtained clients through advertising
- Cardiac cath facility is nearly closed… Dr. Midei is dismissed and later lost his license to practice in MD

HIPAA DATA BREACH

LOSS OF PATIENT HEALTH INFORMATION

- The Health Information Technology for Economic and Clinical Health (HITECH) Act
- Promotes the widespread adoption and standardization of health information technology
- Modifies the HIPAA Privacy, Security, and Enforcement Rules to strengthen the privacy and security protections for health information
- Fines and penalties for data breaches and loss of patient health information (PHI) range from $100 to $50,000 per violation
- The procedures for remediation are more onerous
- Negligent compliance practices may result in fines up to $1.5 million per year
**HITECH & Doctors**

- **What is a Breach?**
  - Acquisition, access, use or disclosure of PHI in a manner not permitted by regulation
  - Compromises the security or privacy of the protected health information
- **Duty to provide notice to patients**
  - "A covered entity shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach." (45 C.F.R § 164.404)

**HITECH**

---

**Doctors & Medical Practices at Risk**

- Lost and/or stolen records containing PHI, including disks, flash drives, and/or laptops that contain PHI
- Viruses
- Inadequate records - physical safeguards
- Disgruntled employees
- Hackers, especially if you treat high profile clients
- Business Associate privacy practices that are insufficient
- Inadequate segregation of duties (those who do not need access to PHI should have no access)

**HITECH**

---

**Your Practice**

- HITECH mandates the timeframe in which the physician practice must act to notify those involved in the PHI breach
  - No more than 60 days after the breach occurred (45 C.F.R. § 164.404(b))
- **What/How?**
  - Brief description of what happened including date of breach and date of discovery
  - Description of the types of PHI involved
  - Steps individuals should take to protect themselves from potential harm
  - Description of what the entity is doing to investigate the breach, to mitigate harm, and to protect against any further breaches
  - Contact information if the individual has questions (45 C.F.R. § 164.404(c))
HITECH
Your Practice

- Duty to provide notice to the government
  - A covered entity shall, following the discovery of a breach of unsecured PHI, notify the Secretary of DHHS
  - For breaches of unsecured PHI involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required... for breaches occurring during the preceding calendar year, in the manner specified on the HHS web site (45 C.F.R. § 164.408)
  - Refer to data elements on HHS website: http://transparency.cit.nih.gov/breach/index.cfm

Breaches Involving 500+ Records

- A breach involving over 500 Patients is more complicated to contain and more costly to resolve.
  - Over 12,000,000 records were exposed in healthcare related breaches in 2009
  - Over 35% of all breaches are caused by a lost laptop
  - 59% of employees leaving their jobs steal information
  - A breach of just 500 records can cost over $100,000 to cure

- You must have an internal and external breach communication plan
  - Your medical practice is exposed to privacy related claims and exposures such as a lost iPad or laptop, rogue employee, hacking or virus attack

Breach Notification Highlights
September 2009 through December 2010

- 14,000* reports of breaches of under 500 patients
- 221 reports involving a breach of over 500 individuals
  - Theft and loss are 67% of large breaches
  - Laptops and other portable storage devices account for 38% of large breaches
  - Paper records account for 21% of breaches

*Note: The asterisk indicates estimated data.
Breach Notification Highlights

500+ Breaches by Type of Breach

- Theft: 51%
- Unauthorized Access: 14%
- Hacking Incident: 10%
- Loss: 5%
- Other: 14%

Breach Notification Highlights

500+ Breaches by Location of Breach

- Laptop: 21%
- Paper Records: 10%
- Other: 10%
- Network Server: 10%
- Email: 10%
- Other: 10%

Typical Action Steps

Large Scale Data Breach

- Consult Legal/Outside Counsel
- Hire IT/Computer Forensic Experts
- Consult a Public Relations/Crisis Communication Firm to develop
  - Communication plan
  - Breach notification letter
  - Public notice for local media
  - News release and Web posting
- Hire a mailhouse for printing, addressing envelopes and mailing letters
- IT/Phone Company to implement toll-free number and email address
- Call center services for patient calls/responses
- Credit monitoring, identity theft and fraud prevention
EMR Concerns: More Lost or Stolen Records

- A significant portion of stimulus funds have been set aside to provide incentives for the digitization of medical records
  - Over $19.2 billion of federal funds are committed to health care IT
  - Beginning in 2011 and continuing through 2014, $17.2 billion in incentive payments will be distributed to eligible healthcare providers
  - Each physician is eligible for up to $44,000 in bonus payments if he/she can demonstrate "meaningful use" EHR before 2015
- HITECH & EMR leaves health care providers with two essential options for protecting records going forward
  - Encrypt electronic health records that contain PHI or
  - Protect against breaches and be prepared to respond in accordance with the mandates of HITECH

Recovery Audit Contractors (RAC) & Post Payment Audits

A MAJOR INTERSECTION

- Healthcare Reform Goals
  - Improve access
  - Provide universal coverage
  - Increase quality reporting to include outcomes
  - Increase integration of care through partnerships of physician networks and hospitals
  - Cost control and cost reduction
- What this means to Administrators
  - Over 70% of healthcare executives surveyed believed that physicians performed inappropriate procedures for monetary benefit
  - Congress is focused on reducing "unnecessary" medical cost
KEY DEFINITIONS

- RAC - Recovery Audit Contractor
- MAC - Medicare Administrative Contractor
- MIC - Medicaid Integrity Contractors
- QIO - Quality Improvement Organizations
- ZPIC - Zone Program Integrity Contractors

RAC Specific Legislation

- 2005 - 2008 RAC Demonstration Program
  - Sec. 302 Tax Relief and Health Care Act (TRHCA) 2006
  - Permanent RAC Program; Reaches Back to 10/01/07
- Current Efforts
  - Healthcare Reform: Expansion of the RACs to Medicaid & Medicare Parts C & D
- Recent Rule 75 Fed. Reg. 69037, 69045 (Nov. 10, 2010)
  - States established Medicaid RAC programs by December 31, 2010
  - State programs were fully implemented April 1, 2011
  - RACs paid on a contingency fee basis

RAC Statistics

- During the implementation phase of the RAC program, over $1.3 billion of improper Medicare payments were found in only five states
  - In full phase, government expects to find over $900 billion of improper payments.
- RAC program is the most aggressive measure taken to date by US government to find and prevent waste, fraud and abuse in medical billing, and recoup monies associated with abusive activities
  - Audit contractors retain 9-12% of payments recovered by the government.
  - RAC audits target both intentional and unintentional overbilling through fines, penalties and restitution charges.
  - RAC auditors are authorized to audit all fee-for-service providers. Any medical provider with a Medicare provider number is at risk.
  - Following RAC audits, subject to appeal rights, a practice has 30 days to pay the government the amount indicated in the audit report. After 30 days, Medicare will automatically deduct owed funds directly from future Medicare payments.
Reasons for RAC Overbilling

- Failure to meet Medicare’s technical & nontechnical standards in performing HCPCS
- Inpatient Outpatient Discrimination
- Other

How Is Over-utilization Detected?

- Zone Program Integrity Contractors (ZPICs)
  - Focus on detecting, deterring & preventing Medicare fraud & abuse
  - May immediately refer to CMS, OIG and/or DOJ/law enforcement
- What triggers a ZPIC audit?
  - High-utilization of services or items
  - High-cost services or items
  - Insufficient documentation
- ZPICs use of statistical sampling & extrapolation
  - Data mining & analysis using databases, statistics, computer analysis & research to predict patterns
- Comparative Billing Reports
  - A snapshot of utilization data for an individual provider
  - Provider billing patterns compared to state & national averages

Preparing Physicians for Audit

- Design a compliance program to facilitate audit success
  - Designate location to receive all audit communication
  - Track audit requests and timeline
  - Trend audit results
  - Communicate with key stakeholders and staff
  - Improve clinical and coding documentation processes
RAC Targets

- Highly Productive Physicians
  - Physicians with annual RVUs > 90th percentile of industry benchmarks
  - Translation: specialties such as cardiology, neurosurgery, orthopedics, et cetera
  - Evaluate your need for additional self audit procedures to evaluate:
    - Medical appropriateness of services
    - Adherence to industry professional standards

CONCLUSIONS

Conclusions

- A major national emphasis on improving quality of care and reducing healthcare costs.
- OIG Investigations of high volume, high cost providers.
- RAC Audits of all outlier providers.
- Heightened public concerns about PHI data breach.
- Stiff Federal data breach penalties.
- Higher risk of data breach than before EHR.
- Plaintiff attorneys are focused on gaining cases from OIG quality and HIPAA data violations.
- Compliance is insurable.
Conclusions – How Doctors Think

- Doctors have good intentions and want to care for patients.
- Computer systems, EMR, and coding take valuable time away from seeing patients.
- Doctors are unsure what information they can disclose and to whom under HIPAA/HITECH rules.
- Data breaches are the farthest thing from their mind.
- Doctors are under extreme practice pressures.
- Doctors want a life too.

Thank You