PHYSICIAN PRACTICE
COMPLIANCE CONFERENCE

October 1–3, 2008 | Philadelphia, PA | Doubletree Hotel Philadelphia

Electronic Medical Record (EMR)

How to Audit the Risks

Schawn Pedersen, CPC, CPC-E/M
Manager
Moss Adams LLP

Health Care Compliance Association
6500 Barrie Road, Suite 250, Minneapolis, MN 55435
888-580-8373 | www.hcca-info.org

Objectives

- Discuss how electronic medical records (EMRs) provide the ability for complete and accurate documentation and quality patient care
- Define the 'Published Legal' Electronic Health Record
- Identify how risk might be introduced into the coding process with functionality available in an EMR
- Consider appropriate actions to support documentation and coding and reduce potential organizational risk

Documentation Essentials

What is documentation and why is it important?

~Medical record documentation is required to record pertinent facts, findings, and observations about an individuals health history

~Chronological documents provide evidence which contributes to the care of the patient and is an important element in providing high quality care

The Medical Record Facilitates

- Ability to evaluate and plan the patient's immediate treatment and to monitor his/her health care over time
- Communication and continuity of care
- Accurate and timely claims review and payment
- Appropriate utilization review and quality of care evaluations
- Data collection for research and education

General Principles of Medical Record Documentation

- The principles of documentation listed are applicable to all types of medical and surgical services in all settings.
- For Evaluation and Management (E/M) services, the nature and amount of physician work and documentation varies by type of service, place of service, and patient status
- Principles may be modified to account for these variable circumstances in providing E/M services

http://www.cms.hhs.gov/MLNProducts/downloads/eval_mgmt_serv_guide.pdf

General Principles of Medical Record Documentation (continued)

- Complete and legible
- Patient encounter should include:
  - Reason for the encounter and relevant history, physical examination findings and prior diagnostic test results
  - Assessment, clinical impression or diagnosis
  - Plan for care
  - Date and legible identity of the observer
- If not documented, the rationale for ordering diagnostic and other ancillary services should be easily inferred

http://www.cms.hhs.gov/MLNProducts/downloads/eval_mgmt_serv_guide.pdf

General Principles of Medical Record Documentation (continued)

- Past and present diagnoses should be accessible to the treating and/or consulting physician
- Appropriate health risk factors should be identified
- The patient's progress, response to and changes in treatment, and revision of diagnosis should be documented
- The CPT and ICD-9-CM codes reported on the health insurance claim form or billing statement should be supported by the documentation in the medical record

http://www.cms.hhs.gov/MLNProducts/downloads/eval_mgmt_serv_guide.pdf

"Published Legal" Health Record

- **Definition AND Importance of the Published Legal Health Record**

"Published Legal" Electronic Health Record

- The health record is a legal business record for the healthcare organization and it must be maintained in a manner that complies with:
  - Applicable regulations
  - Accreditation standards
  - Professional practice standards
  - Legal standards
- Each organization needs to 'define' the *content* of the 'published legal' health records in their organization **and** the *location*

Why is the "Published Legal" Definition Important?

- The EMR is a concept that consists of numerous integrated, component information systems and technologies
  - Some of these systems may be interfaced, some may not
- The electronic files that make up the EMR system consist of different data types, and the data in the files consist of different data formats

NOTE: If the components of the EMR are not defined in the system, the systems they sit in are all at risk!

Criteria Categories for Electronic Medical Records

- Patient Demographics
- Provider Information
- Patient List Management
- Problem Lists
- Allergy Information
- Medication Lists
- Results Access & View
- General Ordering Requirements
- Ordering: Medication Orders
- Medication Reconciliation
- Decision Support for Medication & Immunization Orders
- General Clinical Decision Support
- Medication, Immunization & Blood Products
- Clinical Task Management Assignment
- Capture Patient-Originated Data

How Risk Might be Introduced into the EMR

- **The 5 W's**
- **Types of Risk Associated with EMR**

The 5 “W’s”

- Documentation needed to accurately and completely document and code:
  - Who
  - What
  - When
  - Where
  - Why

Who

- Provider of service versus documenter of service
- Appropriate supervision of ancillary staff
- “Incident to” services - ordering and supervising
- Documentation restrictions for specific elements of evaluation and management services
- Orders

What

- "Cloned" notes - not patient specific - for procedures or E/M services
- Copy versus paste
- Clinical note templates:
  - Leading the provider
- Modifiers
- Advanced Beneficiary Notices

"Dependent upon clinical judgment and nature of presenting problem."

What (continued)

- Addendums
  - Adding "missed" data to complete *documentation* versus adding data to support *coding*
- Diagnostic tests performed during course of encounter and not clearly identify as who provided and when/where provided
- Supplies
- Coding "assistance" via the EMR product itself

When

- Date **and** time
  - Automated or manual entry
  - Date/time stamp configuration
  - Agreement between documentation displayed and audit trail

Where

- Location, location, location!
  - Place of service
  - Physical location
- Modifier assignment

Why

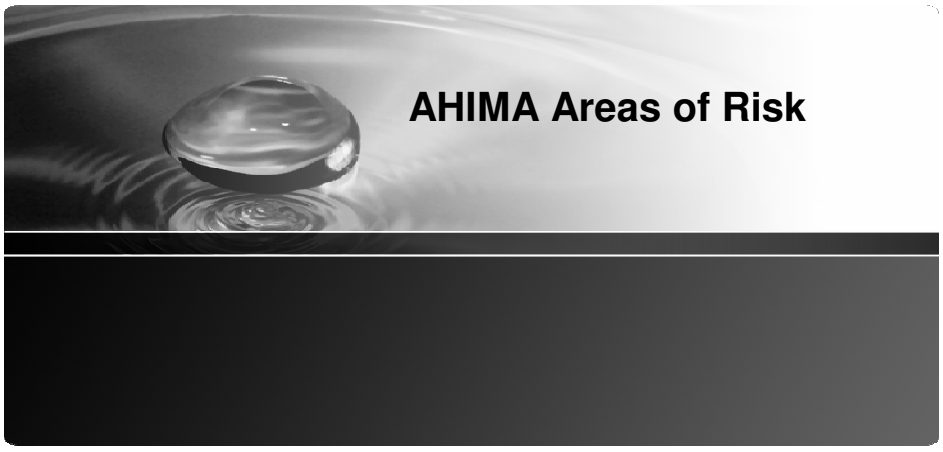
- Medical necessity
  - Potential for overstatement of medical issues
  - “Clinical pathway”
  - Masking of substandard care
- Orders
  - Support of future service provision
- Diagnostic code assignment
  - Diagnostic code order
  - Accuracy of tables provided
  - Shortcuts

Risks Associated with EMR

- Alerts – are they turned on?
- Templates
- Coding ‘Assistance’ (overusing)
- Time Entry – synchronization between systems
- Deleted – is it really deleted?
- Auditing
- Access Control
- Retention

Risks Associated with EMR (continued)

- Authentication and Authorization
  - Passwords – user verification
  - Information attestation
    - Electronic signatures
- Searching and Viewing Records
- Downtime Procedures and Back up
- Printing Medical Records
  - Does your system print all pertinent documentation?
- Metadata
  - eDisclosure
  - eDiscovery



AHIMA Areas of Risk

- What does AHIMA think?
- How does this compare to the five W's?

AHIMA – Areas of Concern

Authorship Integrity Risk:

Borrowing record entries from another source or author and representing or displaying past as current documentation and (in some instances) misrepresenting or inflating the nature and intensity of services provided.

Auditing Integrity Risk:

Inadequate auditing functions that make it impossible to detect when an entry was modified or borrowed from another source and misrepresented as an original entry by an authorized user.

Guidelines for EHR Documentation to Prevent Fraud

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_033097.hcsp

AMIMA – Areas of Concern (continued)

Documentation Integrity Risk:

Automated insertion of clinical data and visit documentation using templates or similar tools with predetermined documentation components with uncontrolled and uncertain clinical relevance.

Patient Identification and Demographic Data Risks:

Automated demographic or registration entries generating erroneous patient identification, leading to patient safety and quality of care issues as well as enabling fraudulent activity involving patient identity theft or providing unjustified care for profit.

What Now?

- You've identified the risks within your EMR system, what now?
  - Develop your next steps!

What Steps to Take?

1. Understand the functionality that exists in the EMR
   - If you've seen one EMR - you've seen one EMR
   - Define your Electronic Health Record and know where it resides in each system
2. Understand the audit trail behind the EMR and how this should be monitored
   - Metadata

What Steps To Take? (continued)

3. Consider where fraud or abuse could be inadvertently introduced by the EMR functionality
4. Develop opportunities to mitigate risk
   - Education and training
   - Necessary policies and procedures
   - EMR "flags," "edits," "alerts," or "soft stops"
   - "Help" features in the EMR
   - Constant auditing, monitoring and feedback
   - "Baseline" coding standards
   - Template design and approval

What Steps To Take? (continued)

5. If not already in place, build a team approach to coding that includes the information systems group, compliance and quality/risk management
6. Communicate all identified concerns
7. Policies and Procedures
   - It isn't enough to write Policies and procedures, they must be enforced

Take Away

- Understand your EMR *or* be involved in the selection/development
  - Evaluate the need for outside assistance with EMR selection
- Clearly define the Electronic Health Record
  - What it is
  - Where it is
- Protect your organization with Policies and Procedures
- Audit
- Enforcement

Thank you for your time!

Schawn Pedersen, CPC, CPC-E/M

Manager

schawn.pedersen@mossadams.com