The Dark Side of the EMR & How to Live With It

HCCA Physician Compliance Conference
Presented by:
Lori Laubach, Partner
Lori-Ann Rickard, Managing Partner

Agenda

☐ What are the risks?
  ■ Internal/external
☐ Going Paperless
  Contingency Plan
☐ Auditing the EMR
☐ Other Risks of the EMR
☐ Case Studies
AHIMA Areas of Concern

What are the risks of the EMR?

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)
AHIMA - Areas of Concern

**Document 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.

**Authorship Integrity**
- Inaccurate representation of authorship of documentation
- Duplication of inapplicable information
- Incorporation of misleading or erroneous documentation due to loss of context that was available to users in the original source
- Ability to take over a record and allow to be the author
- Inclusion of entries from documentation created by others without their knowledge or consent
- Inability to accurately determine services and findings specific to a patient’s encounter
- Inaccurate automated code generation associated with documentation
- Lack of monitoring open patient encounters
- Cut, copy, and paste functionality
- Incident to
Auditing Integrity

- Authentication and amendment/correction issues
- Adding additional text to the same entry
- Auto authentication
- Lack of monitoring activity logs

Documentation Integrity

- Automated insertion of clinical data
- Templates provide clinical information by default and design
- All templates and auto generated entries have the potential to be problematic
- Beneficial feature of EMR is auto population of discrete clinical data
- Problem list maintenance is inconsistent
Patient Identification & Demographics

- Demographic and insurance information may be defaulted for a patient’s encounter
- Patient identity theft is a vulnerable area

External Risks of the EMR

- New opportunities for practitioners to share medical information
  - Helps with documentation and billing
  - Patient management
  - Electronic Prescribing
  - Information exchange

- New opportunities for people with nefarious motives.
  - Viruses
  - Worms
  - Trojan Horses
  - Adware
  - Spyware
Data At Rest

- Where is the data saved/stored?
- Desktop PC’s or Laptops?
- Can data be accessed from home?
- Encryption?

Data In Transit

- Encryption
- Professional IT maintenance and monitoring
Data In Use

- Were is the data accessible from?
  - A secure room, or a room that others can potentially oversee information?
- Is the data accessible to everyone, or only certain users?
- Network security
  - If the information is on a file share, is it secured to prevent transmission to unauthorized users?

Protect Your Computer and Network

- Install a Firewall
- Update your computer regularly
- Implement an anti-virus software package and update it regularly
- Implement an anti-spyware software package and update it regularly
**Educate Users**

- Make sure all users in your practice perform smart computer practices.
- Appoint a security officer to implement your practice’s policy and conduct training.
- Continuously reassess your security procedures and train personnel.
- Prohibit unauthorized computer access within the office.

**Going Paperless**

Paper-based system to an EMR system
Paper-Based Office

- Filing Policies and procedures are often adhered to as closely as possible
- Missing or misfiled information is an ongoing problem
- “To file” piles often contain patient information that is waiting to be inserted into a patient’s file
- Test results arrive in various forms and sizes

Paper-Based Office, Cont.

- Many doctors argue a paper-based office is:
  - Organized;
  - Systematic;
  - Thorough;
  - Efficient; and
  - Legible
EMR/EHR System

- The “paperless” office incorporates:
  - Billing/coding
  - Intra-office communication
  - Appointments
  - Doctor/Patient Interactions
  - Prescriptions
  - Test results
  - Communication with patients

HIPAA

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Requires practices to safeguard patient identities, medical records, and protected health information.

- Health Information Technology for Economic and Clinical Health (HITECH) Act
  - Enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) that was passed February 17, 2009.
HITECH Act & EMR

- Expands the definition of a “Business Associate”
  - HITECH applies directly to business associates
  - Expands and adds new requirements regarding privacy and security

HITECH Act—Penalties

- Civil and Criminal Penalties:
  - Violations apply to business associates in the same manner as a covered entity
Notification Procedures For Breach

- **Covered Entity:**
  - Must notify each individual

- **Business Associate:**
  - Must notify the covered entity

Timeliness of Notification

- Must provide notifications without unreasonable delay
- No later than 60 calendar days after discovery of breach
How To Give Notice

☐ Individual:
  - Written notification by first-class mail
  - To last known address

☐ Mass Media:
  - Allowed if more than 500 unsecured protected health information files are breached

Electronic Copies of Health Information

☐ Individuals are entitled to obtain an electronic copy of their health information

☐ Electronic format is not defined:
  - All Electronic Medical Records are not uniform
Planning the Audit of the EMR

How do I audit the risks of the EMR?

Who to Involve?

- HIM or Medical Records
- Coding personnel
- Clinic Information Systems/Informatics
- Physicians
- Executive Leadership
- Compliance
- You may want to consider:
  - Legal (Attorney Client Privilege)
  - PFS / Finance
Define Scope & Objectives

- Annual risk assessment
- Meet with senior leadership and key EMR process owners
- Question asked of internal audit:
  What are the key factors increasing the EMR risk profile?
  - Technological
  - Behavioral (user)
- AHIMA areas of concern

Fact Finding and Data Gathering

- Obtain & review the following:
  - Policies and procedures related to the EMR
  - Existing documentation and process flows
  - Provider training materials
  - Electronic data – patient encounter information (DOS, CPT, Dx (primary/secondary))
    - Sampling
    - Trending analysis
Interview

What questions should you ask?

Authorship Integrity Q’s

- Does the EHR system have the capability to attribute the entry, modification or deletion of information to a specific individual and/or subsystem?
- Does the EHR system have the capability to use a common date and time stamp across all components of the system?
- How does the system check for duplication and conflicts?
- How does the system track the original unaltered version and edits on a record?
- How does the organization track if a record or report has been altered?
- How does the EHR system provide access control functions?
- Does the organization have P&P’s that define the management of user authentication?
Auditing Integrity Q’s

- Does the EHR system establish a process for logging of all activity on the EHR?
- How long after an entry can the documentation be amended or corrected?
- Does the EHR system preserve data produced in response to a specific request, or can it be recreated reliability?
- How does the audit record maintain the first entry to a medical record?
- Is the record amenable by the original creator or another staff?
- Does the organization have policies that define retention periods and procedures for log records?
- How does the organization know if a record is finalized or completed on the system?

Documentation Integrity Q’s

- Does the organization have P&P’s that specify:
  - Documentation requirements in the EHR?
  - What medical information can be copied from one record to another?
  - What information can be copy forward within a patient’s medical record from one encounter to the next?
  - Define how changes i.e. corrections and amendments are made to all records.
  - Assign responsibility for auditing of log entries and reported exceptions.
- Is editing capability restricted to open versus closed records?
Patient Id & Demographic Accuracy Q’s

- What processes are in place to ensure that the availability of system functionality would not lead to clinical issues not being updated to reflect a clear change in patient’s condition?
  - How is this controlled?
  - How is this monitored?

- What processes are in place to ensure that the availability of system functionality would not lead to or prevent the propagation of misinformation or error?

Sample Work Plans

How do I audit it now?
Audit Procedures - Authorship Integrity

- User access
  - Rights testing
  - Role assignment and security point consistency
- Determine the capability of user login/passwords used simultaneously and different workstations
  - Review user access listing – 1 person – multiple login/passwords?
  - Medical students

Audit Procedures - Auditing Integrity

- Determine EMR editing capability
  - Open versus closed records
  - Create test patient
  - Examine audit logs for audit trail
- EHR capability to use common date/time stamp across all components—test to determine if this can be manipulated in any way either in Epic or in the background.
  - Select one encounter and edit or add information
  - Test date and time stamp
Audit Procedures-Documentation Integrity

What is the volume and timing to closure of typical encounter documentation?

- Obtain and review Patient Billing reports to identify volumes, aging, and types of open encounters
- Select a sample of encounters which are “closed” and have no progress note documentation and determine the amount of time from open to closed timeframe
- Review the EMR and identify if progress notes were written in the correct section

Auditing Specific EMR Functionality

What other items should I consider?
Cut & Paste – Copy & Paste

- Audit Difficulty: Identifying if this function was used
- Documentation Integrity Risk:
  - Bring forth information which is not specific to the patient
  - Fail to edit information that is not applicable to the subsequent encounter
- Utilized software originally designed to detect plagiarism at Universities
- Using encounter data, compared the following EHR
  - Same provider, same primary diagnosis
  - All visits for one day for a provider

AHIMA article: [http://library.ahima.org/xpedio/groups/public/documents/ahima/bok3_005520.hcsp](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok3_005520.hcsp)

Templates

- Identify sample of patient encounters where a template was selected for the encounter documentation. (frequent template users – GI, cardiology, urology, respiratory, and primary care)
- Review EMR documentation to ensure that any default information was verified or updated (patient name, symptoms, medication, etc.)
- Review the EMR audit logs /dark side to ensure that the defaulted information was edited (inquire how this should look prior to examination)
Make me the Author

- Audit Difficulty: Identifying when this function was used
- Test EMR system controls by creating a patient encounter using another provider user ID (or RN) and create documentation
- Review EMR documentation & audit logs (dark side) to ensure that test documentation is attributable to the correct provider
- Turn off / remove this functionality if the EMR doesn’t have the capability to attribute an entry, modification or deletion to a specific individual

Other Risk Areas

What to consider besides what was audited?
General

- Monitoring of coding by EMR is not done
- Assume EMR coding matches billing system
- Coding “assistance” via the EMR product itself (CPT & ICD)
- Coding in EMR is valid although based on pre-determined design

General

- Tracking of user’s changes, deletions or modification to a specific subsystem
- Ability to overwrite another provider if the record is locked
- Lack of policies and procedures related to coding and documentation related to EMR
- Lack of EMR retention policies
Other Issues

- CPT codes “imbedded” in clinical documentation
- Medical necessity
  - Potential for overstatement of medical issues
  - “Clinical pathway” – followed or not
  - Masking of substandard care
- Modifiers
- Abbreviations

Other Issues

- Addendums
- Diagnostic tests performed during course of encounter
  - Not clearly identify as who provided and
  - When & where provided
- Supplies
- Immunizations or other ordered services
Other Issues

- Diagnostic code assignment
  - “Code also”
  - “Code first”
  - Shortcuts
- Multiple encounters being “available” for documentation

Problem List

- Approach development, updates and timely maintenance consistently
- ICD coding & descriptions
  - “attached”
  - “emerge” from documentation
- Identify if multiple diagnoses might be “dropped” into documentation without supporting documentation
- Malpractice concerns
- Avoid “ICD coding” from problem list and not the service documentation
And more. . .

- CPT, HCPCS and ICD codes table maintenance
  - Version controls
  - Update process
  - Testing for effect of updates…information system and coding input into the process
  - Audit trails
  - Timeliness

Case Studies

Scared yet?
Case Study: Malpractice

- Malpractice cases are won and lost by demonstrating humanity of physician through patient interaction.

Case Study: Failure to Backup Records

- Lost records
- Inability to recover data
- Backup power supply
Case Study: Success

- Office efficiencies
- Adaptability
- Focus on patient care
- Remote access

Case Study: Malpractice

Practice lost malpractice case where verdict was over seven figures due to the fact the practice was not able to produce a clear copy of the entire medical record.
Case Study:

- Practice and physicians subject to both corporate and individual liability for failure to accommodate a physician with a disability.

Questions?

Lori Laubach:
lori.laubach@mossadams.com
Lori-Ann Rickard
LARickard@larlegal.com