Auditing an Electronic Medical Record

HCCA's Upper West Coast Regional Annual Conference

Lori Laubach, Partner, Health Care Industry Group, Moss Adams LLP

Teresa Porter, Chief Compliance Officer, UC Davis Health System

December 7, 2012

MOSS ADAMS LLP UCDAVIS HEALTH SYSTEM

Agenda

- Documentation Risk in an EHR
- Confidentiality & Access
- Data Integrity
- Clinical Content
- Meaningful Use
- Auditing or Monitoring

From Testimony of Lewis Morris, OIG

"For example, electronic health records (EHR) may not only facilitate more accurate billing and increased quality of care, but also fraudulent billing. The very aspects of EHRs that make a physician's job easier—cut-and-paste features and templates—can also be used to fabricate information that results in improper payments and leaves inaccurate, and therefore potentially dangerous, information in the patient record. And because the evidence of such improper behavior may be in entirely electronic form, law enforcement will have to develop new investigation techniques to supplement the traditional methods used to examine the authenticity and accuracy of paper records. "

http://oig.hhs.gov/testimony/docs/2011/morris_testimony_07122011.pdf

Warning Letter Issued by US Department of Human Health Services (Sebelius) & Department of Justice (Holder)

On September 24, 2012, CEOs of the Association of Academic Health Centers (AAHC), American Hospital Association (AHA), the Federation of American Hospitals (FAH), the Association of American Medical Colleges (AAMC), and the National Association of Public Hospitals and Health Systems (NAPH), received a letter from HHS Secretary Kathleen Sebelius and Attorney General Eric Holder. The strongly-worded letter raises concerns about reports of the use of electronic health records to improperly bill for services not provided and "upcode" services to receive higher payments than are warranted. The letter puts the whole hospital community on notice that this "misuse" of electronic health records will be aggressively monitored, audited, and prosecuted to the fullest extent of the law. The letter also specifically indicates that CMS will be "reviewing billing through audits" and "initiating more extensive medical reviews to ensure that providers are coding evaluation and management services accurately."

LCD guidance on templates

Noridian Administrative Services, LLC

> Documentation to support services rendered needs to be patient specific and date of service specific. These auto-populated paragraphs provide useful information such as the etiology, standards of practice, and general goals of a particular diagnosis. However, they are generalizations and do not support medically necessary information that correlates to the management of the particular patient. Part B MR is seeing the same auto-populated paragraphs in the HPIs of different patients. Credit cannot be granted for information that is not patient specific and date of service specific.

Source:
https://www.noridianmedicare.com/shared/partb/bulletins/2011/271_jul/Evaluation_and_Management_Services_-_Documentation_and_Level_of_Service_.htm

Documentation Risks AHIMA Areas of Concern

1. Authorship integrity risk: Borrowing record entries from another source or author and representing or displaying past as current documentation, and sometimes misrepresenting or inflating the nature and intensity of services provided
2. 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

Documentation Risks AHIMA Areas of Concern

3. 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

4. Patient identification and demographic data risks: Automated demographic or registration entries generating incorrect 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

Guidelines for EHR Documentation to Prevent Fraud

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

7

1 - Authorship Integrity

- ❑ Inaccurate representation of authorship of documentation
- ❑ Duplication of inapplicable information
- ❑ Incorporation of misleading or wrong documentation due to loss of context for users available from the original source
- ❑ Ability to take over a record and become the author
- ❑ Inclusion of entries from documentation created by others without their knowledge or consent

Authorship Integrity continued…

- 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

Copy and Paste

- Two varieties:
  - Word (Ctrl C)
  - Computer generated
- Concern:
  - Copying and pasting is not noncompliant. It is how the information is used or "counted."
  - For example, per Trailblazer's September 30, 2002, bulletin, Medicare is also concerned that the provider's computerized documentation program defaults to a more extensive history and physical examination than is typically medically necessary to perform, and does not differentiate new findings and changes in a patient's condition."

Copy and Paste

- Real examples:
  - Patient intubated on day one of stay, extubated on day two, however, documentation read for the entire length of stay that "patient intubated" even when the note read that "patient doing well and going home"
  - ED nurse had two records open. She copied part of Patient A's record into Patient B's record—drug use and bi-polar diagnoses showed on Patient B's medical record and billing information
  - In an EMR, the error never truly goes away

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

Approaches

- 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

Plagiarism software download: http://plagiarism.phys.virginia.edu/

AHIMA article:
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok3_005520.hcsp

Auditing of Copy Functionality

Break down the approach by identifying tests by:

- Copy functionalities that originate in software other than the EHR, such as copy in Microsoft Windows
- Copy functionalities that permit duplication of sections of a patient record for use in new documentation, such as medication or problem lists
- Copy functionalities that duplicate an entire prior encounter record from a different date, and possibly from a different author or different patient, and represents it as today's documentation

http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_049706.pdf

13

Another Audit Option

- ❑ Look for inconsistencies within a single note.
- ❑ Conduct an internal audit of at least 20 encounters for a single physician,
- ❑ Run a report in your EHR of all notes in which a physician brought text forward from a previous note.
- ❑ Be particularly vigilant of cloned notes immediately after your go-live date on EHR
- ❑ Keep your compliance department aware of the potential for EHR abuse

14

2 - Auditing Integrity

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

Authentication

Signature serves three main purposes:

- Intent
- Identity
- Integrity

AHIMA EHR Guidelines

1. Access control functions
   a) User authentication
   b) Extensive privilege assignment and control features
2. Capability to attribute the entry, modification or deletion of information to a specific individual or subsystem
3. Capability to log all activity

17

AHIMA EHR Guidelines

4. Capability to synchronize a common date and time across all components of the system
5. Data entry editing
   a) Verify validity of information on entry when possible,
   b) Check for duplication and conflicts
   c) Control and limit automatic creation of information

18

3. Documentation Integrity

- Automated insertion of clinical data
- Templates provide clinical information by default and design
- All templates and auto-generated entries are potentially problematic
- Beneficial feature of EHR is auto population of discrete clinical data
- Problem list maintenance is inconsistent

Templates: A Necessary Evil

- Reminders for important “red flag” questions
- Generate canned phrases, may lose uniqueness.
- One-size-fits-all templates are incomplete, not comprehensive enough, and only work for one problem
- Subjective observations go undocumented
- Medical student and/or resident notes. Linking language by a teaching physician
- Templates drive more unnecessary documentation.

Exploding Notes: Explosive Topic

- Check a box, get a sentence. The same one every time.
- Profoundly troubling
- Exploding notes & Natural Language Processing that reads and assigns code to the automated information
  - Does not sort out Medically Necessary information
  - EHR Assigns code on word quantity not PERTINENCE

Recommendation: Do not implement non-editable canned statements linked to check boxes.

- Most physicians do not enjoy coding or documentation. They embrace shortcuts, not considering compliance risks.
- Your role:
  - Point out these competing tensions: short cuts/compliance
  - Turn up the light, not the heat!
- Mitigate the risk if you do implement note writer functionality
  - Must have the capability to be edited
  - Phrases should be in each provider's own words

21

"Smart Tools" (shortcuts for better documentation)

Smart Sets - Templates for Complete Documentation of Encounter and related procedures or tests

- Allow documentation and coding for entire problem

Smart Text - Problem Specific documentation

- More specific problem/guidance

Smart Phrases - "dot" phrases - common pretexted phrases

- .bmi: (calculates and pulls in last body mass index). .nexheart: (pulls in negative exam for CV system)
- .negneuro: (pulls in negative neuro ROS questions)

22

UCDHS Auditing – Monitoring High Risk Errors

- Implement mandatory compliance reporting of high risk documentation, coding or billing issues
- Compliance is responsible for analyzing and taking the necessary action
  - Isolated or systemic problem
  - Compliance Actions (refund, education, documentation addendums, etc)
  - Report incident to the Documentation Improvement Work Group
- Documentation Work Group (Sub to the Medical Records Committee)
  - Develop policy related to clinical documentation
  - Analyze issues with documentation practices
  - Develop tools to improve documentation
  - Monitor the use of documentation tools
  - Improve clinical documentation

4. Patient Identification & Demographics

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

Patient ID & Demographic Accuracy Questions

- 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?

Patient Identification

- Asset inventory and prioritization
- Threat and vulnerability identification
- Examination of existing security controls associated with addressing identified threats and vulnerabilities
- Determining
  - Likelihood of exposure to identified threats and vulnerabilities
  - Impact (fiscal, workflow, etc.) associated with the exercise of a threat or vulnerability exploitation
- Determining, prioritizing, and mitigating identified risks

Other Risk Areas

Structured Data:	**Free Text:**
☐ Advantages: enables stated values to be supported for specific variables so as to provide standard meaning for reporting purposes (all entries are reportable data) ☐ Disadvantages: Predetermined display names and consistently structured phrases appear the same in all charts; does not allow for descriptions in the clinicians own thoughts or style	☐ Advantages: Preserves the narrative component of the medical record. Each visit appears different because the clinician created it specifically for the individual patient. ☐ Disadvantages: Typing and dictation must be done for each patient by a clinician who would rather be seeing patients than typing. This typing, dictating or filling out templates is very onerous

27

Other Risk Areas

- ❑ 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
- ❑ Tracking of user’s changes, deletions or modification to a specific subsystem
- ❑ Lack of policies and procedures related to coding and documentation related to EHR and retention

28

DATA INTEGRITY

Risks to Data Integrity

- Improper Change Management
  - Metadata
  - Applications, Databases, Operating Systems
- Interface Issues Between Systems
- Inadequate IT Operations

Change Management: Metadata Risk

Pharmacy and Master file

- Mapping and Synchronization of drug database with chargemaster
- Dispensing of drugs in the correct venue of care

Risk

- Fraudulent billing
- Patient Dissatisfaction
- Reputation damage

31

Change Management: Metadata Risk

Lab

- Common Mapping Errors
- Use of “smart sets” within EHR to create custom order sets for provider ease

Risk

- Fraudulent billing
- Patient Dissatisfaction
- Reputation damage

32

Interface Issues Between Systems

Interfaces

- Improper Field-Mapping
- Transmission / Receipt Failure
- Partial Transmission / Receipt Failure
- Processing Failure

Risks

- Data Corruption
- Fraudulent Billing
- Dissatisfied Customers

Confidentiality & Access

Know Where Data is Stored

- Where is the data saved/stored?
- Desktop PC's or Laptops?
- Can data be accessed from home (e.g., PCAnywhere)?
- Portable storage
- Mobile devices
- Encryption?

Data Breaches

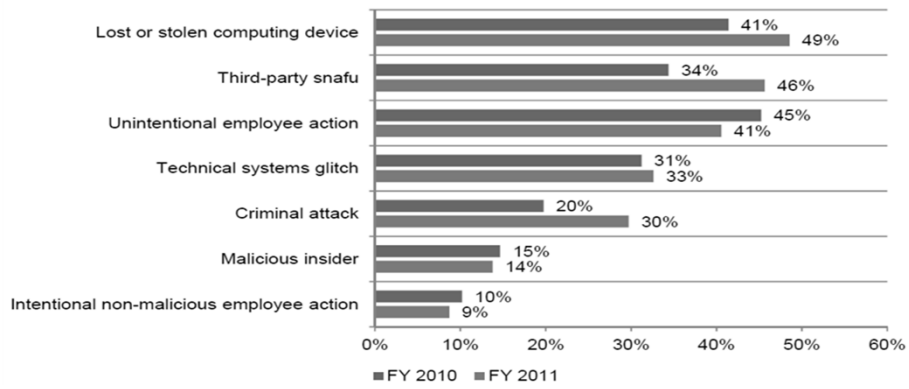
"…the number of *data breaches among healthcare organizations participating in the 2010 and 2011 studies is still growing—eroding patient privacy and contributing to medical identity theft."* *

**Ponemon Institute LLC, Second Annual Benchmark Study on Patient Privacy & Data Security, December 2011*

MOSS ADAMS LLP UCDAVIS HEALTH SYSTEM

Hackers Are Only One Threat

Nature Of Root Causes Of Data Breach Incidents



Ponemon Institute LLC, Second Annual Benchmark Study on Patient Privacy & Data Security, December 2011

37

MOSS ADAMS LLP UCDAVIS HEALTH SYSTEM

Educate Users

Create and maintain an Awareness Program

- Appoint a privacy & security officer to implement your practice's policy and conduct training.
- Make sure all users in you organization perform smart computer practices.
- Continuously reassess your privacy and security procedures and train personnel.
- Ensure you can demonstrate compliance to regulatory agencies

38

Privacy Breach Monitoring Systems

- Systematically identifies users who are engaging in patient access patterns indicative of snooping, identity theft, or other risky behaviors
- Can be performed for all crucial EHRs and applications providing access to Protected Health Information (PHI)
- Filters out known false positives and alerts remaining potential incidents to appropriate privacy personnel
- FairWarning is a leading application in this area

Data Breach Notification Laws

- HIPAA Security Rule- Notice of Breach
  - Requires notification to the US Secretary of Health and Human Services of certain breaches of health information
  - Requires the patient to be informed of certain breaches of protected health information
- California's SB1386
  - Requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed).
- Subsequently, SB 541 & AB 411
  - SB 541 established standards to licensed health facilities mandating reporting to CDPH and patients within 5 days of breach.
    - Potential penalty of up to $25,000 for each patient whose medical information was accessed unlawfully or without authorization and up to $17,500 for each subsequent occurrence of unlawful or unauthorized access of that patient's medical information, subject to a total cap of $250,000.
  - AB 411 created an enforcement body that has authority to investigate potential violations of the AB 211 privacy standards by health care providers.
    - Penalties as provided in the CMIA, ranging from $1,000 to $250,000

MEANINGFUL USE – EHR RISK

ARRA: Qualifying for incentives

"Meaningful Use" criteria must be met

- Divides the requirements into a "core" group of requirements that must be met, plus an additional "menu" of procedures from which providers may choose.
- This "two track" approach ensures that the most basic elements of meaningful EHR use will be met by all providers qualifying for incentive payments, while at the same time allowing latitude in other areas to reflect providers' needs and their individual path to full EHR use.

What criteria affects the EHR?

- ❑CPOE
- ❑Specific data elements
- ❑Security Risk Assessment

Make Meaningful Use Meaningful

Requirement: More than 30% of unique patients with at least one medication in their medication list seen by the EP or admitted to the eligible hospital or CAH have at least one medication entered using CPOE

Options for the display names of the orderable procedures

- Use software's display names

Advantage of creating your own display names:

- Embedded coding hints
  - Add on codes
  - For quantities of J Codes
  - Reminders to give size of lesion

Make Meaningful Use Meaningful

Requirement:

More than 80% of all unique patients seen by the EP or admitted to the eligible hospital or CAH have at least one entry or an indication that no problems are known for the patient recorded as structured data

- "None" is OK but it must be structured text

The compliance issue with Problem Lists not up to date

- Most EHR have a key stroke that loads the Problem List into the Progress Note
- Discrepancies occur as the Problem List diagnosis is not consistent with free text documentation
- Example: Pt is declared free from cancer in the text of the note but the "blown in" Problem List states: Breast Cancer

45

Now let's all head to Hawaii!

Thank You

Lori.laubach@mossadams.com

Teresa.porter@ucdmc.ucdavis.edu

46