ELECTRONIC HEALTH RECORDS - AUDITING QUALITY AND COMPLIANCE

Laura Roberts
Director, Corporate Compliance
Catholic Health East

Amy Bailey Muckler
Principal
HC Healthcare Consulting LLC

OVERVIEW

- Background
- Pros and cons of EHR
- Quality and Patient Safety
- Compliance Risks
- Auditing EHR
- Examples
"Somebody should tell our office manager that a motorized filing cabinet does not qualify as an electronic health record system."

BACKGROUND
A GLIMPSE TO THE FUTURE OF ELECTRONIC RECORDS

- Every provider, in every state, will have the ability to create an EHR for their clients or patients.
- Patients will have the ability to access their entire record with a provider online through patient portals.
- Providers will be able to share patient data electronically and seamlessly.
- Information exchanges will be established to assure continuity of care no matter where the patient is.
- Public health officials will have access to “real time” epidemiology information.
BACKGROUND

○ CMS position on EHR
  • EHRs are the next step in the continued progress of healthcare that can strengthen the relationship between patients and clinicians. The data, and the timeliness and availability of it, will enable providers to make better decisions and provide better care.
  • For example, the EHR can improve patient care by:
    ○ Reducing the incidence of medical error by improving the accuracy and clarity of medical records.
    ○ Making the health information available, reducing duplication of tests, reducing delays in treatment, and patients well informed to take better decisions.
    ○ Reducing medical error by improving the accuracy and clarity of medical records.

PROS AND CONS OF EHR
THE “PROS” OF ELECTRONIC RECORDS

- Improved Patient Safety
  - Quality Core Measures
  - Reduction in errors (legibility, name, patient)
  - Improved measurement of patient outcomes
  - Immediate access = no delay in treatment
  - Access to multiple types of data from a single point

- Increased Continuity of Care
  - Record can potentially follow the patient rather than being re-created at every encounter.
  - Care settings can share patient information allowing for reduced readmissions, better placement, disease management.
  - Providers tend to document for their needs alone; EHR promote consistent communication between providers

THE “PROS” OF ELECTRONIC RECORDS

- Evidence-based Decision Making
  - Readily available data promotes decisions, financial and clinical, based on population specific results.
  - Clinical evidence can be used to provide enhanced patient care

- Evidence-based Reimbursement
  - Coding is based on clearer documentation
  - Enables computer assisted coding
  - Drives Pay for Quality reimbursement

- Greater Patient Engagement
  - Increased access to the record encourages patient “ownership” of their care
THE “CONS” OF ELECTRONIC RECORDS

- Implementation Costs
  - Systems and consistent set up
  - Productivity
  - Provider learning curve
  - Patient care time
- Privacy & Security
  - Potential for breach resulting in large penalties
  - User access/disclosure
  - Stricter definition of secure
- Availability of data
  - Actionable
  - Increased enforcement through automated audits
  - Clinical decisions may be made solely by cost data
  - Security
  - Too much data

THE “CONS” OF ELECTRONIC RECORDS

- They use computers.
  - Downtime/Crashes
  - Virus’
  - User error
  - Imperfect decision making
  - Too formatted due to database type functionality
  - Not human
- LAST BUT NOT LEAST
  - *Increased risk for malpractice and false claims lawsuits*
QUALITY AND PATIENT SAFETY

- Electronic records allow for greater depth and breadth in documentation.
- Conditions can be captured and regularly updated fairly easily.
- Templates may be used to help ensure complete record keeping.
- Prompts may be used to assure due consideration is given to a variety of situations (i.e. capture coverage criteria for devices).
- Quality indicators, such as core measures, are easily captured and reported; increasing likelihood of full reimbursement.
QUALITY AND PATIENT SAFETY

- Reporting of quality indicators is intended to promote enhanced care and long term disease reduction (i.e. smoking cessation, pneumonia vaccine).
- Ease of capturing data, ideally, would allow providers to better reflect the education and care provided.
- However, the easier it is to capture data, the easier it is to capture inaccurate data. Busy providers gravitate toward shortcuts.
- Increased need to audit data, but more difficult to audit due to lack of human abstraction.

QUALITY AND PATIENT SAFETY

- Entry errors are common
  - Provider’s “click” the wrong box
  - System “pulls” data (i.e. test results) incorrectly
- Computerized Physician Order Entry (CPOE) is particularly problematic according to numerous studies. In one survey;
  - 75% of clinical staff indicated they identify multiple errors on a weekly basis.
  - Results in patients receiving the wrong studies and/or services.
  - Standard order sets are templates; providers are used to freedom in orders. May result in over utilization of services.
QUALITY AND PATIENT SAFETY

- Recently in California, 142 nurses from Contra Costa County Hospital filed formal complaints alleging errors in the EHR resulted in medication dosing errors and that the system wouldn’t allow them to document medication administration appropriately.
  - Dosages recommended by the system would have been fatal had they been administered.
- The nurses also complained that their training prior to the EHR implementation was inadequate and incomplete.

QUALITY AND PATIENT SAFETY

- A 47-year old man presented with multiple skin lesions on his arm and back. Dermatology was consulted and performed multiple biopsies.
- Three days later the a PA from the primary care provider’s office looked up the biopsy results in the EHR. The results showed the lesions on the arm and back as benign. The record also showed a diagnosis of melanoma from a biopsy of the thigh. The PA did not see any notations regarding a biopsy of the thigh but went ahead and noted the results in the record and called the patient to inform him of his poor prognosis.
QUALITY AND PATIENT SAFETY

- It was later discovered that the thigh biopsy had been performed on another patient and accidentally entered into the patient’s medical record. The physician and hospital administration met with the patient to disclose the mistake but the patient had already suffered significant emotional distress.

QUALITY AND SAFETY

- What went wrong
  - In this case, neither the Dermatology or pathology providers were fully implemented on the EHR system and had no ability to confirm the results of the biopsy against the rest of the patient’s record to identify the discrepancy.
QUALITY AND PATIENT SAFETY

Dr. A renews a medication, and his e-prescribing program sends an alert advising him that the medication could interact with another drug the patient is taking. He has not prescribed that drug, so his office staff will have to contact the patient to identify who has prescribed it, and then Dr. A will have to contact Dr. X to “negotiate” which drug will be discontinued or changed. If failure to take action results in patient injury from a drug interaction, the doctor may be liable.

- Because of “alert fatigue,” there is a danger that doctors may ignore, override, or disable alerts, warnings, reminders, and embedded practice guidelines. If it can be shown that following an alert or a guideline would have prevented an adverse patient event, the doctor may be found liable for failing to follow it.

QUALITY AND PATIENT SAFETY

- The computer may become a barrier between the doctor and the patient. When the doctor fills in a computer template, it may divert attention from the patient, limit interactive conversation, and restrict creative thinking. This may depersonalize and weaken the doctor-patient relationship. The computer’s location in the office is an important ergonomic consideration; i.e., the location of electrical outlets shouldn’t force you to sit with your back to the patient.
QUALITY AND PATIENT SAFETY

- Many EHRs auto-populate fields in the history and physical (H&P) (from data derived from a prior H&P) and in procedure notes (from personalized or packaged templates). While over-documentation may facilitate billing, entering erroneous or outdated information may increase liability.

- For example, an internist was deposed, and his EHR was the medical record. Some of the auto-populated fields contained obviously wrong information. At deposition, the plaintiff's attorney asked these questions:
  a. “So is the information in this record accurate or not?”
  b. “Do you bother looking at your records?”
  c. “If these ‘auto-populated’ fields are incorrect, can we trust anything in this record?”
  d. “Do you deliver the same level of care as you do in record keeping?”

QUALITY AND PATIENT SAFETY

- Templates with drop down menus facilitate data entry. However, drop down menus are usually integrated with other automated features. An entry error may be perpetuated elsewhere in the EHR—and it may be overlooked, resulting in a new potential for error. Erroneous information, once entered into the EHR, is easily perpetuated and disseminated.

- Vendor contracts may attempt to shift medical liability risks resulting from faulty software design or decision support data onto the doctor. They may also provide that the vendor has rights to utilize patient or provider data. Read all contracts carefully.
QUALITY AND PATIENT SAFETY

Thoughts from a physician at a large institute that recently transitioned to an EHR:

- Chart review during rounds has become nearly worthless noting meaningless repetition in multiple notes while trying to find any indication of new developments. “It’s like Where’s Waldo?”

COMPLIANCE RISKS
FOR EVERY GOOD THING AN EHR OFFERS, THERE IS AN EQUAL AND DIRECTLY RELATED COMPLIANCE RISK.

COMPLIANCE RISKS

- Multiple risks to consider
  - Risks overlap between quality and compliance
    - Medical malpractice
    - Medically unnecessary services
    - HIPAA
    - Cloning
    - Upcoding (Volume of data)
    - EHR generated coding (No qualified human oversight)
    - False claims
  - Concern has been expressed nationwide
    - Specialty colleges
    - Office of Inspector General
    - American Academy of Professional Coders (AAPC)
    - American Health Information Management Association (AHIMA)
On July 12, 2011, Lew Morris, Chief Counsel to the Office of Inspector General testified before a governmental affairs committee on using technology to cut waste and curb fraud in federal health care programs.

- “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 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.”

**2012 OIG Work Plan**

- Evaluation and Management Services: Potentially Inappropriate Payments
  - We will assess the extent to which CMS made potentially inappropriate payments for E/M services and the consistency of E/M medical review determinations. We will also review multiple E/M services for the same providers and beneficiaries to identify electronic health record (EHR) documentation practices associated with potentially improper payments. Medicare contractors have noted an increased frequency of medical records with identical documentation across services.
COMPLIANCE RISKS

- Cigna Government Services stated in June, 2004 in their Part B Medicare Bulletin, “During repeated reviews, we have observed the tendency to “over-document” and consequently to select and bill for a higher level E/M code than medically reasonable and necessary. Word processing software, the electronic medical record, and formatted note systems facilitate the “carry over” and repetitive “fill in” of stored information. Even if a “complete” note is generated, only the medically reasonable and necessary services for the condition of the particular patient at the time of the encounter as documented can be considered when selecting the appropriate level of an E/M service. Information that has no pertinence to the patient’s situation at the specific time cannot be counted.”

- National Government Services stated, “Providers should not bill a higher level when a lower level of service is warranted. The volume of documentation should not be the primary factor upon which a specific level of service is billed.”

COMPLIANCE RISKS

- Palmetto Medicare has stated, “The word cloning refers to documentation that is worded exactly like previous entries. This may also be referred to as ‘cut and paste’ or ‘carried forward’. Cloned documentation may be handwritten, but generally occurs when using a preprinted template or an Electronic Health Record (EHR). While these methods of documenting are acceptable, it would not be expected that the same patient had the exact same problem, symptoms, and required the exact same treatment or the same patient had the same problem/situation on every encounter. Cloned documentation does not meet medical necessity requirements for coverage of services. Identification of this type of documentation will lead to denial of services for lack of medical necessity and recoupment of all overpayments made.”
COMPLIANCE RISKS

- In 2007, AHIMA published “Guidelines for EHR Documentation to Prevent Fraud”
- Journal identified four key areas of concern:
  - Authorship integrity
    - Borrowing record entries from another source of author and representing past as current documentation and (in some instances) misrepresenting the nature and intensity of the services provided.
    - Order authenticity
  - Auditing integrity
    - Inadequate auditing functions that make it impossible to detect when an entry is modified or borrowed from another source and misrepresented as an original entry by an authorized user.

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

- Patient identification and demographic accuracy
  - 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.
COMPLIANCE RISKS

- As with the paper record, the electronic record must be unique to the patient.
- While templates can serve a purpose in assuring complete documentation, they can also hinder accurate documentation.
- If the system is too cumbersome, providers WILL find shortcuts.
  - "If you want me to customize my note for each patient that would take me like 20 extra clicks per patient.”
    - Medical oncologist at a large facility
- The ability to “pull forward” documentation should not replace the need to capture current information.
  - Thoughtful consideration should be given to the amount and type of information that is pulled forward.

COMPLIANCE RISKS

- The provider remains ultimately responsible for all orders, notes, and resulting coding in the electronic record.
  - Most providers will blame “the system” for errors in the record- regardless of whether they have signed off.
  - “Signed but not read” mentality
- All billed services must be documented and supported by the electronic record.
- Be wary of system generated coding and coding prompts
  - Programmed to code based off key words and volume
    - Medical necessity isn’t a factor
    - Significant documentation discrepancies aren’t a factor
  - Are you sure you didn’t review 1 more element from the ROS?
  - If you examined 1 more organ system it could be a 99215
COMPLIANCE RISKS

- EHRs may highlight provider habits or assumptions
  - Individuals completing sections of the record which are only to be documented by the physician (i.e. HPI, Plan, Orders)
  - While coding is based on documentation, not all documentation can be used for coding
  - Significant patient history does not always equal higher level E/M code
  - Timeliness in record completion/sign off

- How much ‘copy and paste’ is acceptable?
- How much differentiation should there be between encounters?
  - Normal physical exams
  - Stable, chronic conditions with no changes required to the treatment plan
- Documentation errors in one record probably mean documentation errors in multiple records.
  - Increase in False Claims Act liability
- Financial incentives to improve quality (documented in EHR) and adopt a meaningfully useful system
  - Increase in False Claims Act liability
**COMPLIANCE RISKS**

<table>
<thead>
<tr>
<th>Paper</th>
<th>Electronic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliance on patient completion of some clinical information</td>
<td>Captured by checkboxes, usually during patient interview</td>
</tr>
<tr>
<td>Provider “short hand”</td>
<td>Standardized language</td>
</tr>
<tr>
<td>Visit specific</td>
<td>Entire history available</td>
</tr>
<tr>
<td>Legibility is sometimes questionable</td>
<td>Always legible</td>
</tr>
<tr>
<td>Not always complete</td>
<td>Not always accurate</td>
</tr>
</tbody>
</table>

**COMPLIANCE RISKS**

- Electronic discovery
  - A whole new host of issues that didn’t exist in the paper world
- Both the government and malpractice lawyers are now looking at “metadata” in addition to printed copies of the EHR to support their cases against providers.
- Metadata includes logon and logoff times, what was reviewed and for how long, what changes or additions were made, and when the changes were made. Smart phone and e-mail records are also discoverable.
- Doctors need to know that all of their interactions with the EHR are time-tracked and discoverable.
AUDITING EHR

AUDITING

- How is the record generated
  - To audit, you need to understand how each aspect of the documentation in the record got there;
    - Prefill
    - Macro
    - Exploding verbiage
    - Copy and paste
    - Pull forward
    - Free form text
    - All of the above
    - Customization by provider
    - Customization by clinic/department
AUDITING

- Regular monitoring of record completion is necessary.
- Each provider should be audited periodically to assure ongoing accuracy.
- Look at your metadata not just the output!
- Use the data available to determine risk areas.
- Look for evidence of cloning – same record, different patients.

AUDITING

- Review for accuracy and reasonableness
  - “I have reviewed the patient’s review of systems, past medical, family and social history.”
    - Is there actually a documented ROS and PFSH in the record?
    - When was the last time it was updated?
    - How long did the provider actually spend reviewing it?
      - 5 minutes, 15 seconds, not at all?
  
- Audit access logs
- Trend Evaluation and Management codes
- Use audit results to provide regular and tangible feedback to providers
SUMMARY AND RECOMMENDATIONS

RECOMMENDATIONS

The following recommendations were made to HHS to ensure data accuracy and implement reasonable safeguards against fraud.

- Establish policies; educate; enforce
- Audit
  - Functions and Features
    - User access (person, time, place, location)
- Provider identification
  - Unique identification to isolate entries in the record
- User access authorization
  - Sophisticated user ID/Password system to prevent unauthorized access
- Documentation process
  - All entries should be date/time stamped
  - Identify methods for entry- voice, copy/paste, typed, import
RECOMMENDATIONS

- Evaluation and Management Coding
  - Users require to valid entries that support level of service

- Proxy authors
  - Entries made by other than the licensed provider should clearly identify the date, time, author and content entered

- Record modification after signature
  - Maintain before and after copies

- Auditor access
  - View only access, relevant/necessary portions

- EHR traceability
  - Tracking numbers to documents

- Patient involvement in anti-fraud
  - Patients should have access to their records

- Patient identity proofing
  - Verification of patient identity to prevent medical identity theft

- Structured and coded data
  - Data is maintained in a manner to allow for analysis to identify and prevent fraud

- Integrity of EHR transmissions
  - Standard, recognized methods to ensure accurate transmissions

- Accurate linkage of claims to clinical records
  - Audit trail from the EHR to the billing system
**RECOMMENDATIONS**

- Frequent auditing and consistent monitoring
- Proactively identify problematic data entry shortcuts
- Educate users
  - One-to-one provider training
  - Use real time chart examples
  - Shadow providers, compare to electronic note
- Encourage open communication between providers, coders, billers and compliance
- Promote and facilitate communications between IT and the end users
- Development of internal controls and policies and procedures to reduce the risk of falsification and improper use

**QUESTIONS**
CONTACT INFORMATION

- Laura Roberts
  Director, Corporate Compliance
  Catholic Health East
  lroberts1@che.org
  (610) 550-3200

- Amy Bailey Muckler, CHC, CPC, CPC-H, CPC-I, CCS-P
  Principal
  HC Healthcare Consulting LLLC
  aballey@hchealthcareconsultingllc.com
  (208) 489-2539

RESOURCES

- CMS Electronic Health Records

- 2012 OIG Work Plan

- AHIMA
  - www.ahima.org