Health IT Due-Diligence and Risk Mitigation

Dr. Reed D. Gelzer
Provider Resources, Inc.
June 22, 2016
Adapted from: EHR Systems’ Fraud Potential
Recognizing and leveraging counterfeit care records

If your vetting process simply assumes a credible-appearing record, they now have an app for that.
Biography in Brief

Reed D. Gelzer, MD, MPH

Co-Chair, HL7 EHR Standards Workgroup
Co-Facilitator, HL7 Records Management and Evidentiary Support WG
Member, Sedona Conference Working Group 1 (Digital Evidence)
Internist, Clinical Practice 1986-1997
Specialist/Consultant on EHR Systems 2000-2016
EHR Certification (CCHIT) 2006-2009 (pre-”Meaningful Use”)
Objectives

Participants will gain or reinforce understanding of:

1. The concept of clinical records as business records,

2. The unique vulnerabilities of EHRs that can raise your risk of legal and economic losses,

3. How to “screen” your EHR for risk, and

4. How to mitigate risk.
Maintaining Legally Sound Records (Oversimplified)

“Federal Rules of Evidence (803(6)) and the Uniform Business and Public Records Act adopted by most states allow exception to the hearsay rule for records maintained in the regular course of business, including health records. All records must be identified and authenticated prior to admissibility in court.”

Adapted from AHIMA e-HIM Work Group on Maintaining the Legal EHR. "Update: Maintaining a Legally Sound Health Record—Paper and Electronic." Journal of AHIMA 76, no.10 (November-December 2005): 64A-L.
A record must have been:

• Documented in the normal course of business (following normal routines)
• Kept in the regular course of business
• Made at or near the time of the matter recorded
• Made by a person within the business with knowledge of the acts, events, conditions, opinions, or diagnoses appearing in it
...Legally Sound

- Type of computer used and its acceptance as standard and efficient equipment
- The record’s method of operation
- The method and circumstances of preparation of the record, including:
  - The sources of information on which it is based
  - The procedures for entering information into and retrieving information from the computer
  - The controls and checks used as well as the tests made to ensure the accuracy and reliability of the record
  - The information has not been altered
...Sound

The sources of information on which it is based

Who actually provided the service?

Who actually authored the record?
...Sound

The procedures for entering information into and retrieving information from the computer

Copied? “Cloned?” Boilerplated? (identical for multiple encounters, multiple patients)
...Sound

The controls and checks used as well as the tests made to ensure the accuracy and reliability of the record

Nonsense Records?
...Sound

The information has not been altered

Amended records clearly indicated?

Audit log functions enabled at all times?
Objectives

Participants will gain or reinforce understanding of:

1. The concept of clinical records as business records,

2. The unique vulnerabilities of EHRs that can raise your risk of legal and economic losses,

3. How to “screen” your EHR for risk, and

4. How to mitigate risk.
Current EHR Systems Requirements

- CMS Documentation Guidelines for E&M Services? No
- Accurately reflect who provided the service? No
- Identify an altered record? No
- Associate authors with each’s contribution to a record? No
- Accurate Release of Information responses? No
- Require 24/7/365 Operational Audit Capabilities? No
Counterfeiting
Emergency Department record with falsified physical examination

#1 EHR vulnerability is clinical notes, all types, all users
PHYSICAL EXAM

CONSTITUTIONAL: Patient is afebrile, Vital signs reviewed, Alert and oriented X 3, Patient has mild pain distress. (01:37 JG)

HEAD: Atraumatic, Normocephalic. (01:38 JG)

EYES: Eyes are normal to inspection. Pupils equal, round and reactive to light, No discharge from eyes. Extraocular muscles intact, Sclera are normal, Conjunctiva are normal. (01:38 JG)

ENT: Posterior pharynx normal, Mouth normal to inspection. (01:38 JG)

NECK: No meningeal signs, Cervical spine nontender. (01:38 JG)

RESPIRATORY CHEST: Chest is nontender, Breath sounds normal, No respiratory distress. (01:37 JG)

CARDIOVASCULAR: RRR, No murmurs. (01:37 JG)

ABDOMEN: Abdomen is non–tender, No masses, No pulsatile masses, No distension, No peritoneal signs, No hernias, McBurney’s point, non tender. Liver and spleen normal. (01:37 JG)

BACK: There is no CVA Tenderness, There is no tenderness to palpation, Normal inspection. (01:37 JG)

UPPER EXTREMITY: Inspection normal, No cyanosis, No clubbing, No edema, Normal range of motion. (01:38 JG)

LOWER EXTREMITY: Inspection normal, No cyanosis, No clubbing, No edema, Normal range of motion, No calf tenderness. (01:38 JG)

NEURO: GCS is 15, No focal motor deficits, No focal sensory deficits, Speech normal. (01:38 JG)

SKIN: Skin is warm, Skin is dry. (01:38 JG)

PSYCHIATRIC: Oriented X 3, Normal affect. (01:38 JG)
Audit Level: 3  Recommended Level: 5  Chart needs more documentation

Correct Deficiencies...
System > Auditing

System level auditing / reporting
Centrify logs many user activities for audit/reporting purposes. Use these settings to expand the scope of the actions permanently stored to the database.

Caution: Enabling these options will increase database storage requirements.
- Audit running of inquiries
- Audit previewing, printing and faxing of non-confidential reports and documents
- Audit changing of flowsheet views
- Audit viewing of non-confidential documents

Document level contribution logging
Centrify always logs user name and time when modifications are made to a chart document. Use the following settings to store details about clinical data contributions/modifications.

Caution: Enabling this option will increase database storage requirements.
- Log clinical data contributions to documents
  - Log only the most recent value when a user corrects their own entry
  - Do not save previous versions of modifications to text in the chart note
  - Do not log Encounter Form changes that modify Document Temp Symbols
    (Usually non-clinical data changes such as comments and button selections that produce translation text)
“In a decision that is poised to have resonating implications for health services providers, the Supreme Court of the United States explicitly endorsed the “implied false certification theory of liability” under the False Claims Act (FCA) in Universal Health Services, Inc. v. U.S. ex rel. Escobar.”

http://healthlawsidebar.com/?p=1701
EHRs: Due Diligence Required

Currently there are no regulatory or “Certification” requirements that address EHR fitness for use as clinical or business records (or patient safety).

Use is at your own risk
EHRs: Due Diligence Required

Wildly variable in their ability to support authentic patient records,

Configuration and use dependent
EHRs: Due Diligence Required

Record end-users, including payers, medical defense attorneys, and plaintiff’s attorneys, as well as judges are becoming increasingly attentive to EHR “vulnerabilities”

Clinicians themselves remain primarily responsible for assuring that their EHR Systems will stand up to legal scrutiny as well as clinical fitness
Objectives

Participants will gain or reinforce understanding of:

1. The concept of clinical records as business records,

2. The unique vulnerabilities of EHRs that can raise your risk of legal and economic losses,

3. How to “screen” your EHR for risk, and

4. How to mitigate risk.
Key Risk Points:

• EHR configuration options with no legitimate purpose
• Dubious EHR “tools” that have legitimate alternatives
• What does your EHR System’s “Release of Information” output look like?
• When an audit log is requested, what will you send?
• (When a patient requests an access audit report, showing who has created, edited, or viewed their records, what will you provide to them?)
1. If your EHR has a training module where you can “play” with it, that’s best for initial testing.

2. If no training module, create an unmistakably fake patient.

   Ex: John Doe Fake-Female-Born 1816, Age 200
Testing: A Simple Scenario

Ideally your system has supports two authors

1. Author 1 captures part of an encounter record. If a template or form is commonly used, use that.
2. If Copy or “Bring Forward” or similar functions are available for citing previous an already-existing record, use that function.
3. Author 1 exits the record, authenticating or “signing” it if that function is available.
4. Author 1, either as part of step 3 or as step 4, conveys the in-progress record to Author 2.
Testing: A Simple Scenario

5. Author 2 “signs into” the encounter, effectively picking up where Author 1 left off.
6. Author 2 alters some of Author 1’s content
7. Author 2 adds content.
8. Author 2 completes the record and goes through all steps to close and authenticate the record.
Testing: A Simple Scenario

9. Author 2 exits that patient record.
10. Author 2 calls up the same record and views it, then again exits.
11. Author 2 calls up the same record once again and this time executes an amendment to the record, changing some elements of the content, then re-authenticates, signs, and exits the record.
1. View the episode of care record and also print it.
2. Does the screen view show that you are looking at an altered (amended) record? Does the printed one?
3. Does the screen view show both authors and which author did what? Does the printed one?
4. If one or the other (or both) does not show each author and each’s contributions, figure out what you would have to do to see and reconstruct that (may require the audit log)
Testing: Simple Analysis

5. Can you see what Author 1 did originally that was then altered by Author 2?

6. Can you view or print an audit log?
   • If so, what does it show for the use of the template or form?
   • Does it show that all the template’s components were entered at the same exact time or does it show that the components were entered sequentially?
   • Does it accurately show which author did what and show that Author 2 changed Author 1 content?

Note: If no audit log, that’s a different problem.
Objectives

Participants will gain or reinforce understanding of:

1. The concept of clinical records as business records,
2. The unique vulnerabilities of EHRs that can raise your risk of legal and economic losses,
3. How to “screen” your EHR for risk, and
4. How to mitigate risk.
If you don’t have a policy and procedure manual for your clinical records, how will you know if your EHR System supports, complies?
#1 Risk Mitigation: Medical Records P&P

1. Who can create?
2. Who can view?
3. Who can authenticate?
4. Who can amend?
5. Documentation tools:
6. CODING COPIED ENTRIES
#1 Risk Mitigation: Medical Records P&P

5. Documentation tools:
   - Templates: Pre-populated or null (blank)?
   - Copy functions (including “bring forward”) attribution?
   - Record entries attributed accurately?
   - Editing others’ entries?
#1 Risk Mitigation: Medical Records P&P

1. Record entries attributed accurately?
2. Amended records unmistakably marked “Amended”?
3. What does your EHR “signature” actually do?

- Do not bypass security (shared passwords, etc.)
- Make sure your EHR blocks users from unauthorized view access
Clinicians themselves remain primarily responsible for assuring that their EHR Systems will stand up to legal scrutiny.
Questions?

Reed D. Gelzer, MD, MPH
Co-Chair, HL7 EHR Standards Workgroup
Co-Facilitator, HL7 Records Management and Evidentiary Support Workgroup
Provider Resources, Inc.
Newbury, NH
Philadelphia, PA
203-506-5361
Record Corruption: No Audit = No Integrity

HIPAA Security Rule: System must produce a report that shows who accessed record and when, including who contributed to the record

Audit Log absent or insufficient means:

- **Impeachable**: Cannot validate authenticity (who or what actually authored and when, for which patient)
- **Cannot assess** whether the record was not altered after it was originally created
- **Cannot reconstruct** originals from altered records
“Medical-Legal Cases That Went South” by Dr. Keith Klein, HIMSS 2015.


Gelzer, Reed, “Record Entry Origination: Risks that lurk in your EHR for confirmation of the who, what, where, and when of patient care,” in New Perspectives, Volume 34, Fall 2015.

EHR Records Risk Assessments
An Evolving Use of the EHR System Functional Model Standard

HIMSS HL7
April 15, 2015

Reed D. Gelzer, MD, MPH
Co-Chair, HL7 EHR Workgroup
Co-Facilitator, HL7 EHR Records Management and Evidentiary Support Workgroup
and HL7 EHR/Security Vocabulary Alignment Workgroup
Provider Resources, Inc.
What is to be done?

HL7 EHR-System Functional Model, Release 2

April 2014

Sponsored by:
Electronic Health Records Working Group